UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

TECSEC, INCORPORATED,

Plaintiff,

v.

INTERNATIONAL BUSINESS MACHINES CORPORATION, SAS INSTITUTE INC., SAP AMERICA, INC., SAP AG, CISCO SYSTEMS, INC., SUN MICROSYSTEMS, INC., SYBASE, INC., SOFTWARE AG, SOFTWARE AG, INC., ADOBE SYSTEMS INCORPORATED, EBAY INC., PAYPAL, INC., and ORACLE CORPORATION,

Defendants.

Case No. 1:10-cv-00115-LMB-TCB

IBM'S BRIEF IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT OF INEQUITABLE CONDUCT AND INVALIDITY

PUBLIC VERSION

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Other Authorities

Defendant International Business Machines Corporation ("IBM") respectfully submits this Brief in Support of its Motion for Summary Judgment of Inequitable Conduct and Invalidity.

INTRODUCTION

TecSec brought this action against IBM and 12 other defendants on February 5, 2010, for alleged infringement of U.S. Patent Nos. 5,369,702 ("the '702 patent"); 5,680,452 ("the '452 patent"); 5,717,755 ("the '755 patent"); 5,898,781 ("the '781 patent") (collectively, "the '702 patent family"); 6,694,433 ("the '433 patent"); and 7,069,448 ("the '448 patent"), among others.[1] (D.I. 1.) On August 16, 2010, IBM filed its amended answer and counterclaims alleging, among other things, that the '702 patent family is unenforceable due to inequitable conduct committed by the applicant and his attorneys before the United States Patent and Trademark Office ("PTO"), and that the '433 and '448 patents are invalid. (D.I. 281 at ¶¶ 215, 227–266.) Discovery is now closed and there is no genuine dispute of material fact concerning these defenses. Summary judgment should thus be granted in favor of IBM.

As discussed below, TecSec's inequitable conduct stems from its efforts to steal technology developed by Roy D. Follendore, III ("Follendore") by secretly filing a patent application directed to his technology in the name of Follendore's intern, M. Greg Shanton ("Shanton"). Follendore joined TecSec soon after it was founded by Ed Scheidt ("Scheidt") in 1991. He brought to TecSec his ideas and software relating to object-oriented encryption, and worked on refining his ***o***bject-***o***riented ***key*** ***man***agement technology (called "OOKeyMan") pursuant to a verbal agreement with Scheidt that he would receive a percentage of the proceeds. In connection with his work, Follendore filed his '707 patent application with the help of

[1] TecSec originally asserted 11 patents, but dismissed 5 of those patents shortly before serving expert reports because it had no basis for asserting infringement.

attorneys Jon L. Roberts ("Roberts") and Thomas Champagne ("Champagne").

But TecSec was struggling at the time. Roberts took over as president of TecSec and cancelled Follendore's proceeds-sharing agreement with Scheidt. A year-long dispute between Follendore and TecSec concerning inventorship and ownership of the object-oriented encryption technology erupted, with Follendore insisting that he should be named as an inventor on any patent applications that TecSec might file related to his OOKeyMan software.

During the course of this dispute, Roberts conspired with Shanton, Champagne, and Scheidt to steal Follendore's inventions and cut Follendore out of any financial interest in the company. In furtherance thereof, Shanton, Roberts, and Champagne secretly filed a patent application (which ultimately led to the '702 patent family) with Shanton named as the sole inventor, directed towards the OOKeyMan software that Follendore had been developing for well over a year. Despite the fact that the OOKeyMan software existed long before—at least as early as 1992—Shanton told the PTO that he first conceived of it two weeks after Follendore left the company, on September 29, 1993, holding himself out to be the sole inventor. In addition, Roberts and Champagne copied large portions of a patent claim from Follendore's earlier-filed '707 patent application, yet told the PTO that Shanton was the sole inventor of the copied claim.

These efforts to falsely claim inventorship by Shanton and to conceal Follendore's inventorship claims constitute inequitable conduct by Shanton, Roberts, and Champagne. As discussed below, the inequitable conduct by these individuals included:

(i) withholding their copying from Follendore's earlier patent claim;

(ii) withholding Follendore's inventorship assertions and the litigation about those assertions;

(iii) withholding the fact that the OOKeyMan software existed long before Shanton claims to have invented it; and

(iv) submitting false declarations asserting that Shanton was the sole inventor of the ’702 patent family claims.

Each of these misrepresentations and omissions was made for the express purpose of deceiving the PTO into believing that Shanton was the sole inventor of the OOKeyMan software and ’702 patent family claims, in furtherance of TecSec’s plan to steal Follendore’s technology. Each of the patents of the ’702 patent family are therefore unenforceable as a matter of law.

And, as further discussed below, there is also no genuine dispute that the remaining patents-in-suit, the ’433 patent and the ’448 patent, are invalid over the prior art. The Court should therefore enter summary judgment in favor of IBM as set forth below.

STATEMENT OF UNDISPUTED MATERIAL FACTS

I. Undisputed Facts Relating To The ’702 Patent Family Inequitable Conduct.

1. The application that led to Follendore’s ’707 patent (“the ’707 patent application”) was filed with the PTO on January 27, 1993. (Exs. A1–A2.)[2]

2. The ’707 patent application was assigned to Examiner Cangialosi at the PTO and prosecuted by attorneys Roberts and Champagne. (Exs. A1–A2.)

3. The applications that led to Shanton’s ’702 patent, ’755 patent, ’452 patent, and ’781 patent (“the ’702 patent family applications”) were filed with the PTO on October 18, 1993, September 13, 1994, February 24, 1995, and September 10, 1997, respectively. (Exs. A3–A10.)

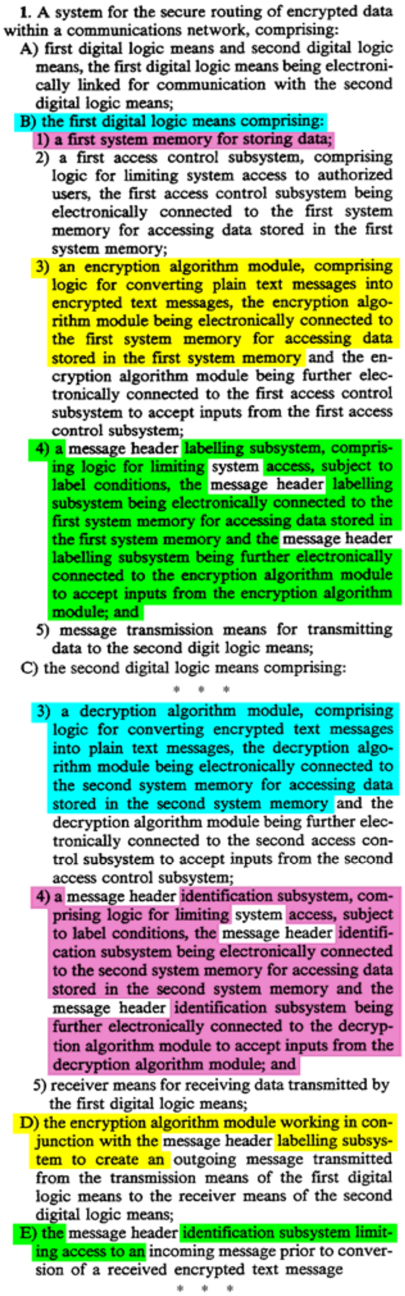
4. All of the ’702 patent family applications were assigned to Examiner Gregory at the PTO and prosecuted by attorneys Roberts and/or Champagne. (Exs. A3–A10.)

5. Each of the ’702 patent family applications includes one claim that was substantially copied verbatim from Follendore’s earlier-filed ’707 patent application claim 1,

[2] Exhibits are attached to the declaration of Jeanne M. Heffernan, filed concurrently herewith.

including claim 8 of the ’702 patent, and claim 14 of the ’755, ’452, and ’781 patents.

U.S. Patent No. 5,369,707 (Follendore)



1. A system for the secure routing of encrypted data within a communications network, comprising:

A) first digital logic means and second digital logic means, the first digital logic means being electronically linked for communication with the second digital logic means;

B) the first digital logic means comprising:

1) a first system memory for storing data;

2) a first access control subsystem, comprising logic for limiting system access to authorized users, the first access control subsystem being electronically connected to the first system memory for accessing data stored in the first system memory;

3) an encryption algorithm module, comprising logic for converting plain text messages into encrypted text messages, the encryption algorithm module being electronically connected to the first system memory for accessing data stored in the first system memory and the encryption algorithm module being further electronically connected to the first access control subsystem to accept inputs from the first access control subsystem;

4) a message header labelling subsystem, comprising logic for limiting system access, subject to label conditions, the message header labelling subsystem being electronically connected to the first system memory for accessing data stored in the first system memory and the message header labelling subsystem being further electronically connected to the encryption algorithm module to accept inputs from the encryption algorithm module; and

5) message transmission means for transmitting data to the second digit logic means;

C) the second digital logic means comprising:

* * *

3) a decryption algorithm module, comprising logic for converting encrypted text messages into plain text messages, the decryption algorithm module being electronically connected to the second system memory for accessing data stored in the second system memory and the decryption algorithm module being further electronically connected to the second access control subsystem to accept inputs from the second access control subsystem;

4) a message header identification subsystem, comprising logic for limiting system access, subject to label conditions, the message header identification subsystem being electronically connected to the second system memory for accessing data stored in the second system memory and the message header identification subsystem being further electronically connected to the decryption algorithm module to accept inputs from the decryption algorithm module; and

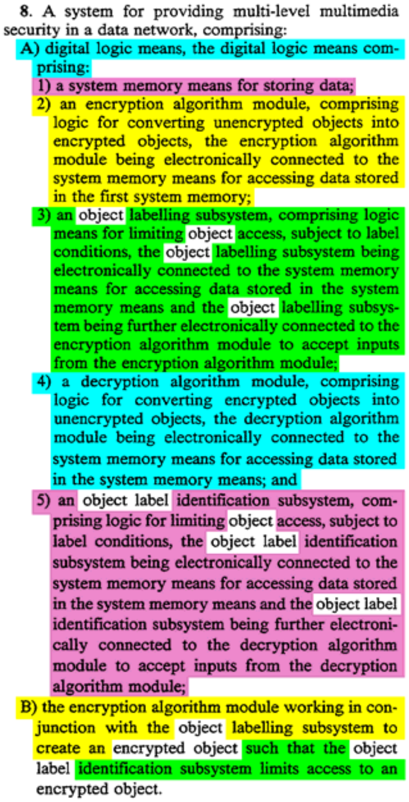
5) receiver means for receiving data transmitted by the first digital logic means;

D) the encryption algorithm module working in conjunction with the message header labelling subsystem to create an outgoing message transmitted from the transmission means of the first digital logic means to the receiver means of the second digital logic means;

E) the message header identification subsystem limiting access to an incoming message prior to conversion of a received encrypted text message

* * *

U.S. Patent No. 5,369,702 (Shanton)



8. A system for providing multi-level multimedia security in a data network, comprising:

A) digital logic means, the digital logic means comprising:

1) a system memory means for storing data;

2) an encryption algorithm module, comprising logic for converting unencrypted objects into encrypted objects, the encryption algorithm module being electronically connected to the system memory means for accessing data stored in the first system memory;

3) an object labelling subsystem, comprising logic means for limiting object access, subject to label conditions, the object labelling subsystem being electronically connected to the system memory means for accessing data stored in the system memory means and the object labelling subsystem being further electronically connected to the encryption algorithm module to accept inputs from the encryption algorithm module;

4) a decryption algorithm module, comprising logic for converting encrypted objects into unencrypted objects, the decryption algorithm module being electronically connected to the system memory means for accessing data stored in the system memory means; and

5) an object label identification subsystem, comprising logic for limiting object access, subject to label conditions, the object label identification subsystem being electronically connected to the system memory means for accessing data stored in the system memory means and the object label identification subsystem being further electronically connected to the decryption algorithm module to accept inputs from the decryption algorithm module;

B) the encryption algorithm module working in conjunction with the object labelling subsystem to create an encrypted object such that the object label identification subsystem limits access to an encrypted object.

(Ex. A11 (matching elements shown in respective highlighted colors); *see also* Exs. A2–A10.)

6. Neither Shanton nor his attorneys Roberts and Champagne informed the PTO that they had copied substantial portions of claim 1 of Follendore’s ’707 patent into claims of the ’702, ’755, ’452, and ’781 patent applications. (Exs. A7–A10.)

7. The ’702, ’755, and ’781 patents refer to “the present invention” as “the Distributed Cryptographic Object Method (‘DCOM’)” and state that “[t]he current implementation of the DCOM at the application layer is called the Object-Oriented Key Manager (OOKeyMan).” (Ex. A3 at 5:18–19, 6:40–42; Ex. A4 at 5:16–17, 6:35–37; Ex. A6 at 4:38–39, 5:58–60.) The ’452 patent similarly refers to “[t]he present invention” as “the Distributed Cryptographic Object Method (‘DCOM’)” and states that “[t]he preferred implementation of the present invention at the application layer is OOKeyMan®.” (Ex. A5 at 8:3–4, 9:24–25.)

8. TecSec and Shanton assert that Shanton conceived of OOKeyMan and the inventions of the ’702 patent family on September 29, 1993, two weeks after Follendore left the company. (Ex. A12; Ex. A13 at HK2005629; Ex. A14 at 145:2–146:17, 155:18–156:9, 168:19–21; Ex. A15 at 256:11–20; Ex. A16.)

9. OOKeyMan existed before September 29, 1993. (Ex. A17; Ex. A14 at 165:5–166:24, 176:7–181:19; Ex. A18; Ex. A19 at 2; Ex. A20 at HK0025543–45; Ex. A21 at 302:15–305:24; Ex. A22; Ex. A23 at 230:18–237:11; Ex. A24 at HK2025208; Ex. A25 at TEC01769324, TEC01769337; Ex. A26; Ex. A27; Exs. A41-A42; Exs. A55–A57.)

10. Neither Shanton nor his attorneys Roberts and Champagne disclosed to the PTO the prior existence of OOKeyMan. (Exs. A7–A10.)

11. From at least October 13, 1993, to at least August 22, 1994, Follendore claimed inventorship in OOKeyMan in correspondence with Roberts, specifically stating that he should be named as an inventor on any patent applications TecSec might file on OOKeyMan. (Exs. A29–A39; *see also* Ex. A21 at 232:12–299:18.)

12. On October 18, 1993, four business days after Roberts understood that Follendore asserted an inventorship claim in OOKeyMan, Roberts and Champagne filed the ’702 patent

application naming Shanton as the sole inventor. (Ex. A7.)

13. Neither Shanton nor his attorneys Roberts and Champagne disclosed to the PTO that Follendore had made a claim of inventorship over the purported subject matter of the ’702 patent application. (Exs. A7–A10.)

14. On May 18, 1994, TecSec filed an action against Follendore in the U.S. District Court for the Eastern District of Virginia, Civil Action No. 94-646-A, in response to Follendore’s claims of inventorship. (Ex. A38.)

15. TecSec and Follendore settled the dispute in August 1994, and agreed that “TECSEC shall pay the sum of Forty-Two Thousand Five Hundred Dollars ($42,500.00) to Follendore” and that “TECSEC will acquire all right, title and interest in NetShield, Ookeyman, NLU or crypto engine software … ***only*** upon final payment.” (Ex. A39 at ¶¶ 1, 6.)[3]

16. Neither Shanton nor his attorneys Roberts and Champagne disclosed to the PTO the litigation or settlement between TecSec and Follendore. (Exs. A7–A10.)

17. On October 15, 1993, Shanton signed a declaration representing, among other things, that: (i) “I believe I am the original, first and sole inventor of the subject matter which is claimed”; (ii) “I acknowledge the duty to disclose information which is material to the examination”; and (iii) “I declare that all statements made herein of my own knowledge are true … and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.” This declaration was submitted to the

[3] All emphasis added unless otherwise noted.

PTO during prosecution of the ’702, ’755, and ’781 patent applications. (Ex. A7 at IBMTS-00000219–20; Ex. A8 at IBMTS002635993–94; Ex. A10 at IBMTS002636166–67.)

18. On February 10, 1995, Shanton signed a declaration representing, among other things, that: (i) “I believe I am the original, first, and sole inventor of the subject matter which is claimed”; (ii) “I acknowledge the duty to disclose information which is material to the examination”; and (iii) “I declare that all statements made herein of my own knowledge are true … and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.” This declaration was submitted to the PTO during prosecution of the ’452 patent application. (Ex. A9 at IBMTS-002635789–90.)

19. TecSec has provided no explanation for (1) the failure to inform the PTO about: the copying of Follendore’s ’707 patent claim 1; Follendore’s inventorship assertions and the resulting litigation against Follendore; the prior existence of the OOKeyMan software; or (2) the affirmative act of submitting Shanton’s false declarations claiming to be the sole inventor of the ’702 patent family claims. (Ex. A40 at 9–12.)

II. Undisputed Facts Relating To The ’433 Patent Invalidity.

20. The ’433 patent to Kolouch issued on February 17, 2004, from an application filed on October 20, 1999. (Ex. B1.)

21. TecSec contends that the inventions contained in the ’433 patent were conceived of by James L. Kolouch in or about April 1999. (Ex. B3 at 7.)

22. U.S. Patent No. 7,010,681 to Fletcher *et al.* (“Fletcher”) issued on March 7, 2006, from an application filed on January 29, 1999. (Ex. B2.)

23. Fletcher is prior art to the ’433 patent under 35 U.S.C. § 102(e). (Ex. B1; Ex. B2; Ex. B3 at 7.)

24. Fletcher was not considered by the PTO during examination of the application that issued as the ’433 patent. (Ex. B1.)

25. Fletcher discloses every limitation of claims 1–8 and 10–11 of the ’433 patent. (Ex. B1; Ex. B2; Ex. B4.)

26. Claim 9 of the ’433 patent depends from claim 8 and requires that “wherein the other syntax is of another Extensible Markup Language.” (Ex. B1 at 8:34–35.)

27. Claim 12 of the ’433 patent depends from claim 11 and requires that “wherein the other syntax is of another Extensible Markup Language.” (Ex. B1 at 8:58–59.)

28. The application filed on October 20, 1999, that led to the ’433 patent did not disclose “another Extensible Markup Language” as claimed by claims 9 and 12 of the ’433 patent. (Ex. B5; Ex. B6 at 25; Ex. B7 at 29.)

III. Undisputed Facts Relating To The ’448 Patent Invalidity.

29. The ’448 patent to Odell *et al*. issued on June 27, 2006, from an application filed on December 5, 2002. The ’448 patent claims priority to a provisional application filed on December 5, 2001. (Ex. C1.)

30. TecSec contends that the subject matter of the ’448 patent was invented in or about September 2001. (Ex. B3 at 7.)

31. U.S. Patent No. 7,600,131 to Krishna *et al*. (“Krishna”) issued on October 6, 2009, from an application filed on July 6, 2000. (Ex. C2.)

32. Krishna is prior art to the ’448 patent under 35 U.S.C. § 102(e). (Ex. C1; Ex. C2; Ex. B3 at 7.)

33. Krishna was not considered by the PTO during examination of the application that issued as the ’448 patent. (Ex. C1.)

34. Krishna discloses every limitation of claims 1–18 of the ’448 patent. (Ex. C1; Ex. C2; Ex. C3.)

ARGUMENT

I. Legal Standards.

A. Summary Judgment.

Summary judgment should be entered where “the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(c)(2); *see also Haulbrook v. Michelin N. Am., Inc.*, 252 F.3d 696, 702 (4th Cir. 2001). Summary judgment “is properly regarded not as a disfavored procedural shortcut, but rather as an integral part of the Federal Rules as a whole, which are designed to secure the just, speedy, and inexpensive determination of every action.” *Celotex Corp. v. Catrett*, 477 U.S. 317, 327 (1986) (citation omitted). Summary judgment is not avoided simply because there is some “metaphysical doubt” as to the material facts. *Matsushita Elec. Indus. v. Zenith Radio Corp.*, 475 U.S. 574, 586 (1986). The nonmoving party (here, TecSec) must set forth the existence of a genuine issue for trial such that a reasonable finder of fact can return a verdict for that party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). “[U]nsupported or conclusory averments are insufficient to avoid summary judgment where the moving party has met its initial burden.” *TechSearch, L.L.C. v. Intel Corp.*, 286 F.3d 1360, 1372 (Fed. Cir. 2002) (citation omitted); *see also Sitrick v. Dreamworks, LLC*, 516 F.3d 993, 1001 (Fed. Cir. 2008) (“Conclusory expert assertions cannot raise triable issues of material fact on summary judgment.”).

B. Inequitable Conduct.

Patent applicants and their attorneys have a duty to prosecute patent applications in the PTO with candor, good faith, and honesty. *Advanced Magnetic Closures, Inc. v. Rome Fastener Corp.*, 607 F.3d 817, 829 (Fed. Cir. 2010); 37 C.F.R. § 1.56(a). A party asserting inequitable conduct must prove by clear and convincing evidence that the applicant or his attorneys breached the duty by (1) failing to disclose material information or submitting materially false information with (2) an intent to mislead or deceive the examiner. *Advanced Magnetic*, 607 F.3d at 829.

"As a critical requirement for obtaining a patent, inventorship is material." *Id*. at 830, *quoting PerSeptive Biosystems, Inc. v. Pharmacia Biotech, Inc.*, 225 F.3d 1315, 1321 (Fed. Cir. 2000). Any questions concerning inventorship are therefore material and must be raised with the examiner, ***irrespective*** of how the examiner may ultimately decide the issue. *See Leviton Mfg. Co. v. Universal Sec. Instruments, Inc.*, 606 F.3d 1353, 1360 (Fed. Cir. 2010) ("[W]hether the inventorship of the patents as issued is correct does not determine the materiality of the statements in this case, just as whether concealed prior art would actually invalidate the patent is irrelevant to materiality." (citation omitted)). It follows, therefore, that concealing another's involvement in the conception of the invention is inequitable conduct. *Frank's Casing Crew & Rental Tools, Inc. v. PMR Techs., Ltd.*, 292 F.3d 1363, 1376 (Fed. Cir. 2002). Likewise, copying claims from another's patent application is material and must be brought to the attention of the examiner. *Leviton*, 606 F.3d at 1360 ("Had the examiner been aware that different Leviton employees each claimed to be first inventors of the same subject matter recited in the same claims, it would have raised serious questions regarding inventorship—an issue that is clearly material to patentability.").

"Under the intent prong, a party can prove intent to deceive the PTO based on direct evidence or on circumstantial evidence 'with the collection of inferences permitting a confident judgment that deceit has occurred.'" *Advanced Magnetic*, 607 F.3d at 829 (citation omitted). "Intent rarely can be, and need not be, proven by direct evidence. Instead, an intent to deceive is usually inferred from the facts and circumstances surrounding the conduct at issue." *Cargill, Inc. v. Canbra Foods, Ltd.*, 476 F.3d 1359, 1364 (Fed. Cir. 2007) (citations omitted); *see also Leviton*, 606 F.3d at 1362. Moreover, "in the absence of a credible explanation, intent to deceive ***is generally inferred*** from the facts and circumstances surrounding a knowing failure to disclose material information." *Bruno Indep. Living Aids, Inc. v. Acorn Mobility Servs., Ltd.*, 394 F.3d 1348, 1354 (Fed. Cir. 2005); *see also Ferring B.V. v. Barr Labs., Inc.*, 437 F.3d 1181, 1191 (Fed. Cir. 2006). "Suffice it to say that we have recognized … that summary judgment is appropriate on the issue of intent if there has been a failure to supply highly material information and if the summary judgment record establishes that (1) the applicant knew of the information; (2) the applicant knew or should have known of the materiality of the information; and (3) the applicant has not provided a credible explanation for the withholding." *Ferring*, 437 F.3d at 1191.

C. Invalidity Based Upon Anticipation Under 35 U.S.C. § 102(e).

An alleged invention must be new to meet the requirements of patentability. *See C.R. Bard, Inc. v. M3 Sys., Inc.*, 157 F.3d 1340, 1349 (Fed. Cir. 1998). Under 35 U.S.C. § 102(e):

> A person shall be entitled to a patent unless – ...
>
> > (e) the invention was described in ... a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent ...

"A claim is anticipated under 35 U.S.C. 102 'if each and every limitation is found either expressly or inherently in a single prior art reference.'" *IPXL Holdings, L.L.C. v. Amazon.com, Inc.*, 430 F.3d 1377, 1381 (Fed. Cir. 2005) (citation omitted). Although each claim is presumed valid, 35 U.S.C. § 282, the presumption is not conclusive and, when a prior art reference was not cited to the PTO during prosecution, the movant may more easily carry its burden. *See Sibia*

Neurosciences, Inc. v. Cadus Pharma. Corp., 225 F.3d 1349, 1355–56 (Fed. Cir. 2000); *EWP Corp. v. Reliance Universal, Inc.*, 755 F.2d 898, 905 (Fed. Cir. 1985). Although anticipation is a question of fact, it may be decided on summary judgment where, as here, there is no genuine dispute as to material facts. *See Gen. Elec. Co. v. Nintendo Co.*, 179 F.3d 1350, 1353 (Fed. Cir. 1999); *SmithKline Beecham Corp. v. Apotex Corp.*, 403 F.3d 1331, 1343 (Fed. Cir. 2005) ("[W]ithout genuine factual disputes underlying the anticipation inquiry, the issue is ripe for judgment as a matter of law.").

D. Invalidity For Failure To Comply With The Written Description Requirement Of 35 U.S.C. § 112 ¶ 1.

Section 112, paragraph 1 of the Patent Act requires that "[t]he specification shall contain a written description of the invention." 35 U.S.C. § 112 ¶ 1. "[T]he purpose of the written description requirement is to 'ensure that the scope of the right to exclude, as set forth in the claims, does not overreach the scope of the inventor's contribution to the field of art as described in the patent specification.'" *Univ. of Rochester v. G.D. Searle & Co.*, 358 F.3d 916, 920 (Fed. Cir. 2004) (citation omitted). "This requirement protects the *quid pro quo* between inventors and the public, whereby the public receives 'meaningful disclosure in exchange for being excluded from practicing the invention for a limited period of time.'" *ICU Med., Inc. v. Alaris Med. Sys., Inc.*, 558 F.3d 1368, 1377 (Fed. Cir. 2009) (citation omitted).

"Compliance with the written description requirement is a question of fact but is amenable to summary judgment in cases where no reasonable fact finder could return a verdict for the non-moving party." *PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1307 (Fed. Cir. 2008). "To satisfy the written description requirement, a patent applicant must 'convey with reasonable clarity to those skilled in the art that, as of the filing date sought, he or she was in possession of the invention. The invention is, for purposes of the 'written description' inquiry, whatever is now claimed.'" *ICU Med.*, 558 F.3d at 1377 (citation omitted). "Such description need not recite the claimed invention *in haec verba* but must do more than merely disclose that which would render the claimed invention obvious." *Id.* "***[A]ll the limitations must appear in the specification***. The question is not whether a claimed invention is an obvious variant of that which is disclosed in the specification." *Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1572 (Fed. Cir. 1997); *see also Tronzo v. Biomet, Inc.*, 156 F.3d 1154, 1158 (Fed. Cir. 1998) ("[T]he disclosure must describe the claimed invention with all its limitations.").

II. The '702 Patent Family Is Unenforceable Because Of Inequitable Conduct By Shanton And His Attorneys Roberts And Champagne.

A. Background Of The Inventorship Dispute.

1. The Development Of The "OOKeyMan" Software.

Follendore began his career with the military and CIA. (Ex. A28 at 7:20–46:16; Ex. A58–A59.) During this time, he obtained experience in cryptography and communications security, and came up with ideas regarding object-oriented encryption. (*Id.*; *see also* Ex. A28 at 34:2–36:1, 52:8–11.) He also met Scheidt, and later joined Scheidt at TecSec in about August 1991, shortly after Scheidt founded the company. (Ex. A28 at 38:9–47:6.)

While at TecSec, Follendore further developed his ideas concerning object-oriented encryption into a product called NetShield and the underlying object-oriented key management software that he called "OOKeyMan." (*Id.* at 98:6–100:22; Ex. A23 at 203:5–205:1, 218:14–222:5.) As part of this development, in approximately June 1992, Follendore wrote "A 2020 View Of Multimedia INFOSEC" (Ex. A28 at 65:17–68:8; Ex. A41; Ex. A42), in which he described ways of providing multi-level security to multimedia objects (Ex. A42 at HK2025038) and advocated object-oriented encryption (*id.* at HK2025065 ("Object oriented operating systems will be the vehicle for true multimedia security…"), HK2025068).

About a year after Follendore joined TecSec, TecSec hired Shanton as an intern to help Follendore with his work. (Ex. A14 at 38:9–42:9; Ex. A28 at 48:6–50:13.) At the time, Shanton was a college student working as a clerk in a software retail store. (Ex. A14 at 38:9–42:9; Ex. A28 at 48:6–50:13.) He had no experience in encryption, but was knowledgeable about software packages that could assist Follendore in his product development. (Ex. A14 at 32:25–33:4, 38:9–42:9; Ex. A28 at 49:18–50:10, 52:13–53:18, 129:22–130:13.) Shanton thereafter assisted Follendore with the NetShield product development, including the OOKeyMan software, during 1992 and 1993. (Ex. A14 at 43:10–46:2; Ex. A28 at 129:22–130:13.) During this time, Follendore filed his ’707 patent application with the help of Roberts and Champagne. (Exs. A1–A2.)

[redacted]

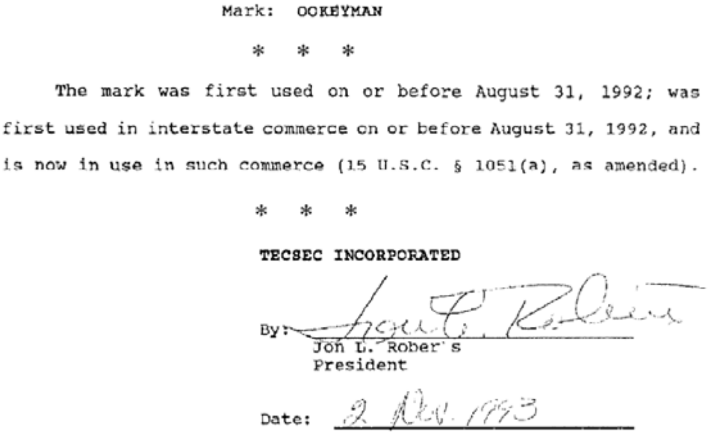
[redacted]

[redacted]

[redacted]

[redacted]

[redacted] Similarly, TecSec's president and prosecuting attorney, Roberts, applied for a trademark on "OOKeyMan," by swearing to the PTO that the trademark "was first used in interstate commerce on or before August 31, 1992":



Mark: OOKEYMAN

* * *

The mark was first used on or before August 31, 1992; was first used in interstate commerce on or before August 31, 1992, and is now in use in such commerce (15 U.S.C. § 1051(a), as amended).

* * *

TECSEC INCORPORATED

By: ____________________
Jon L. Rober's
President

Date: 2 Nov. 1993

(Ex. A20 at HK0025543–45; *see also* Ex. A21 at 302:15–305:24.)

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

2. Follendore's Dispute With TecSec Concerning Inventorship Of And Rights To The OOKeyMan Software.

[redacted]

[redacted]

[redacted]

[redacted]

Immediately after receiving the October 13, 1993, draft settlement, Roberts, Shanton, and Champagne set upon a course of conduct at the PTO designed to steal Follendore's technology and conceal the true inventorship of OOKeyMan:

- On October 14, 1993, Shanton executed a disclosure document claiming that he alone invented OOKeyMan, "the current implementation" of the "present invention." He claimed to have conceived of the invention on September 29, 1993, approximately two weeks after Follendore left the company. (Ex. A13.)
- On October 15, 1993, Shanton signed a declaration swearing that he is the "first and sole inventor of the subject matter which is claimed and for which a patent is sought" in the '702 patent application. (Ex. A7 at IBMTS-00000219–20.)
- On October 18, 1993, the next business day, Champagne filed the '702 patent application under Roberts' direction. (Ex. A7 at IBMTS-00000195–222; Ex. A21 at

104:6–13.) The application included Shanton's sole-inventorship declaration. (Ex. A7 at IBMTS00000219–20.)

- On May 3, 1994, without alerting the PTO, Shanton's attorneys copied substantial portions of Follendore's earlier-filed '707 patent claim 1 into new claim 8 of Shanton's '702 patent application. (Ex. A7 at IBMTS00000255–269.) And they later copied this same claim language into each of the other patents of the '702 patent family. (Exs. A4–A6.)

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

B. Shanton And His Attorneys Withheld Highly Material Information From The Examiner During Prosecution Of The ’702 Patent Family And Submitted Shanton’s False Declarations Claiming To Be The Sole Inventor.

1. Shanton And His Attorneys Withheld The Fact That They Copied Substantial Portions Of Follendore’s ’707 Patent Application Claim 1 Into The ’702 Patent Family Claims.

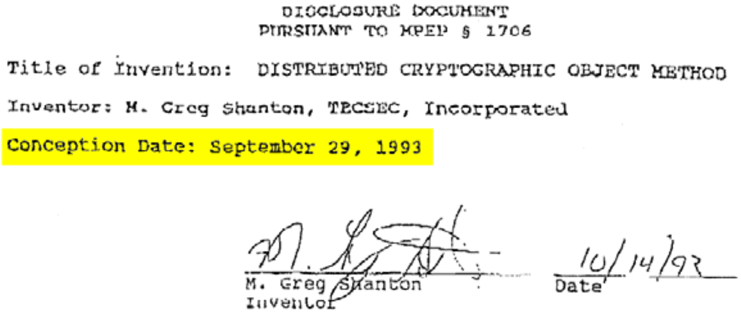
As illustrated in Ex. A11, the vast majority of claim 8 of the ’702 patent, and claim 14 of the ’755, ’452, and ’781 patents were copied verbatim from claim 1 of Follendore’s earlier-filed ’707 patent application. Yet neither Shanton nor his attorneys told the PTO that they had copied Follendore’s claim. (Exs. A7–A10.)

Because of the likely impact on inventorship, which is “a critical requirement for obtaining a patent,” *Advanced Magnetic*, 607 F.3d at 830, the Federal Circuit has held that copying claims in this way is material and must be brought to the attention of the examiner:

> ***The copying of certain claims from the Germain application with one set of named inventors into the ’766 patent application with another set of inventors suggests that the named inventors may not have, in fact, invented the claimed subject matter.*** Here, Leviton submitted patent applications and sworn inventorship declarations from two different sets of inventors, both attesting that they were inventors of the claimed subject matter. ***Had the examiner been aware that different***

> ***Leviton employees each claimed to be first inventors of the same subject matter recited in the same claims, it would have raised serious questions regarding inventorship—an issue that is clearly material to patentability.*** Moreover, as we have acknowledged, "whether the inventorship of the patents as issued is correct does not determine the materiality of the statements in this case, just as whether concealed prior art would actually invalidate the patent is irrelevant to materiality."

Leviton, 606 F.3d at 1360 (citation omitted). This is especially true here, because there is no dispute that Shanton did ***not*** come up with the inventions of the '702 patent family at the time of the earlier Follendore '707 application that he copied—Shanton told the PTO that he did not conceive of his invention until September 29, 1993, nearly eight months ***after*** Follendore filed his '707 patent application on January 27, 1993:



DISCLOSURE DOCUMENT
PURSUANT TO MPEP § 1706

Title of Invention: DISTRIBUTED CRYPTOGRAPHIC OBJECT METHOD

Inventor: M. Greg Shanton, TECSEC, Incorporated

Conception Date: September 29, 1993

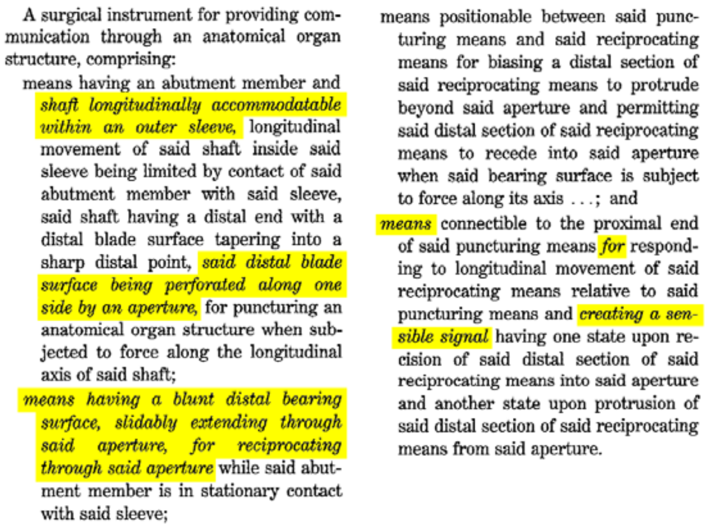
M. Greg Shanton
Inventor

10/14/93
Date

(Ex. A13; Ex. A1.) Yet the law is clear that "[n]either an inventor nor his counsel may graft claims onto an earlier specification if those claims do not reflect what the inventor actually invented at the time of the earlier application." *Leviton*, 606 F.3d at 1360.

Moreover, even if ***Follendore*** was not the ***sole*** inventor of the '702 patent family, the copied claims demonstrate that Follendore was at a very minimum a joint inventor under 35 U.S.C. § 116. "'[T]he critical question … is who conceived … the subject matter of the ***claims*** at issue.'" *Frank's Casing*, 292 F.3d at 1373, *quoting Ethicon, Inc. v. U.S. Surgical Corp.*, 135 F.3d 1456, 1460 (Fed. Cir. 1998). Accordingly, "[t]o determine whether [a person] made a contribution to the conception of the subject matter of [the claim] this court must determine what [the person's] contribution was and then whether that contribution's role appears in the ***claimed invention***." *Ethicon*, 135 F.3d at 1461; *see also Frank's Casing*, 292 F.3d at 1373. As illustrated in Ex. A11, Follendore clearly contributed all, or at least a substantial portion of, the claimed subject matter. (*See also* Ex. A10 at 206:24–219:11.) Indeed, the Federal Circuit has found much less contribution requires finding a person a joint inventor:

In Ethicon, the Federal Circuit found that a person was a joint inventor because he contributed the following highlighted concepts to the claimed invention:



A surgical instrument for providing communication through an anatomical organ structure, comprising:

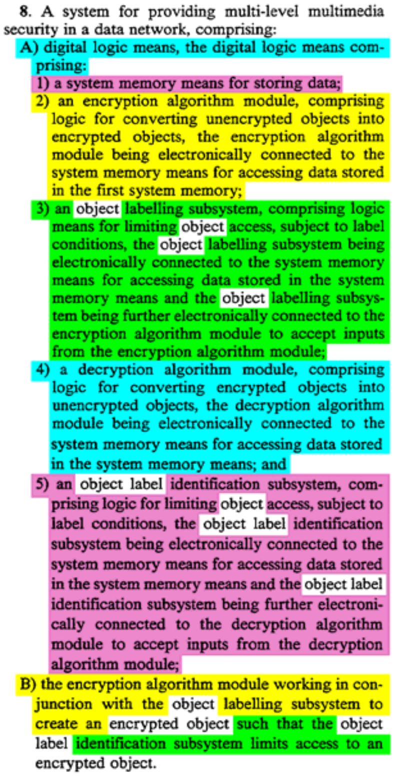
means having an abutment member and *shaft longitudinally accommodatable within an outer sleeve,* longitudinal movement of said shaft inside said sleeve being limited by contact of said abutment member with said sleeve, said shaft having a distal end with a distal blade surface tapering into a sharp distal point, *said distal blade surface being perforated along one side by an aperture,* for puncturing an anatomical organ structure when subjected to force along the longitudinal axis of said shaft;

means having a blunt distal bearing surface, slidably extending through said aperture, for reciprocating through said aperture while said abutment member is in stationary contact with said sleeve;

means positionable between said puncturing means and said reciprocating means for biasing a distal section of said reciprocating means to protrude beyond said aperture and permitting said distal section of said reciprocating means to recede into said aperture when said bearing surface is subject to force along its axis . . .; and

means connectible to the proximal end of said puncturing means *for* responding to longitudinal movement of said reciprocating means relative to said puncturing means and *creating a sensible signal* having one state upon recision of said distal section of said reciprocating means into said aperture and another state upon protrusion of said distal section of said reciprocating means from said aperture.

In this case, Shanton and his attorneys copied the following highlighted language from Follendore's '707 application:[4]



8. A system for providing multi-level multimedia security in a data network, comprising:

A) digital logic means, the digital logic means comprising:

1) a system memory means for storing data;

2) an encryption algorithm module, comprising logic for converting unencrypted objects into encrypted objects, the encryption algorithm module being electronically connected to the system memory means for accessing data stored in the first system memory;

3) an object labelling subsystem, comprising logic means for limiting object access, subject to label conditions, the object labelling subsystem being electronically connected to the system memory means for accessing data stored in the system memory means and the object labelling subsystem being further electronically connected to the encryption algorithm module to accept inputs from the encryption algorithm module;

4) a decryption algorithm module, comprising logic for converting encrypted objects into unencrypted objects, the decryption algorithm module being electronically connected to the system memory means for accessing data stored in the system memory means; and

5) an object label identification subsystem, comprising logic for limiting object access, subject to label conditions, the object label identification subsystem being electronically connected to the system memory means for accessing data stored in the system memory means and the object label identification subsystem being further electronically connected to the decryption algorithm module to accept inputs from the decryption algorithm module;

B) the encryption algorithm module working in conjunction with the object labelling subsystem to create an encrypted object such that the object label identification subsystem limits access to an encrypted object.

[4] Even the few terms not copied directly from Follendore's claims were nonetheless disclosed by the Follendore '707 patent. For example, the '707 patent discloses "multilevel multimedia" security. (Ex. A1 at 2:3–8.) And the "message" or "message header" disclosed in the '707 patent is an example of an "object." (Ex. A3 at 3:42–4:10; [redacted] So replacing the term "message header" in claim 1 of the '707 patent with the term "object" in the '702 patent family was nothing new.

Ethicon, 135 F.3d at 1461; *see also* Ex. A11. At a minimum, therefore, Follendore was a joint inventor on each of the ’702 patent family applications. *See Ethicon*, 135 F.3d at 1460 (“Furthermore, a co-inventor need not make a contribution to every claim of a patent. *See* 35 U.S.C. § 116. A contribution to one claim is enough.”).

Accordingly, Shanton and his attorneys were obligated to inform the examiner that they had copied large portions of Follendore’s claim 1 so that the examiner could determine whether or not Follendore should have been included as either the sole or a joint inventor on each of the ’702 patent family applications. “Even if the examiner might have ultimately concluded that [the named inventors on the later patent] invented the claimed subject matter, the nearly identical claims raise a substantial inventorship question that would have required additional investigation by the examiner. Thus, we hold that [the patentee’s] failure to disclose the [earlier] application during the prosecution of the [later] patent was material.” *Leviton*, 606 F.3d at 1360.

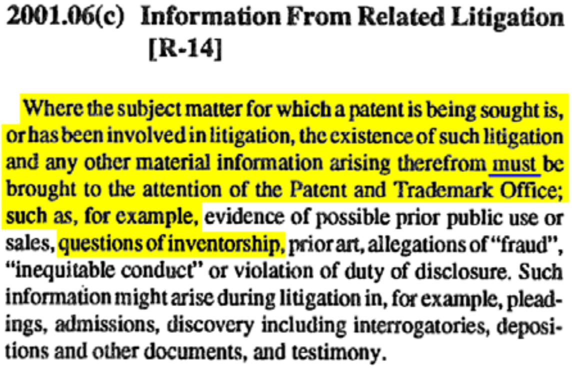
2. Shanton And His Attorneys Withheld Follendore’s Inventorship Claim And The Litigation About That Claim.

[redacted]

[redacted]

Even more stark, however, was Roberts' total failure to disclose the litigation about inventorship between Follendore and TecSec—Roberts cannot claim that he was unaware of that. Yet neither he, Champagne, nor Shanton informed the PTO about that litigation. TecSec brought the lawsuit in direct response to Follendore's inventorship and ownership claims in OOKeyMan. (*See* Exs. A31–32; Ex. A38.) Significantly, the agreement settling the litigation dealt directly with Follendore's claims in OOKeyMan (Ex. A39 at ¶ 6 ("TecSec ***will acquire*** all right, title and interest in NetShield, OOKeyMan").) That the complaint does not refer to the

’702 patent application by number is not surprising—the application was secret, although Follendore anticipated that such an application would be filed. (Ex. A31 at HK2025648.) Failure to disclose the OOKeyMan lawsuit to the PTO was material. As stated in the MPEP:



2001.06(c) Information From Related Litigation [R-14]

Where the subject matter for which a patent is being sought is, or has been involved in litigation, the existence of such litigation and any other material information arising therefrom must be brought to the attention of the Patent and Trademark Office; such as, for example, evidence of possible prior public use or sales, questions of inventorship, prior art, allegations of “fraud”, “inequitable conduct” or violation of duty of disclosure. Such information might arise during litigation in, for example, pleadings, admissions, discovery including interrogatories, depositions and other documents, and testimony.

(MPEP § 2001.06(c), 5th ed. rev. 15 (Aug. 1993); *see also* Ex. A54 at 39:14–40:21; Carmichael Decl. Ex. A at ¶ 262.)

It is undisputed that inventorship is *per se* material. (Ex. A54 at 29:22–25, 113:3–6.) The repeated failure of Roberts, Champagne, and Shanton to disclose Follendore’s inventorship claims to the examiner, their decision not to investigate Follendore’s claims, and their failure to disclose the resulting litigation to the examiner, were thus highly material to the patentability of the claims of the ’702 patent family. *See PerSeptive Biosystems*, 225 F.3d at 1320–22 (inventorship, and information about inventorship, is material); *Advanced Magnetic*, 607 F.3d at 830 (“As a critical requirement for obtaining a patent, inventorship is material.”).

3. Shanton And His Attorneys Withheld The Fact That OOKeyMan—Which Shanton Characterized As The “Current Implementation” Of His Invention—Existed And Was Created By Follendore Long Before Shanton’s Alleged Invention.

Shanton told the PTO on October 14, 1993, that his conception date for the ’702 patent family was September 29, 1993, two weeks after Follendore left TecSec. (Ex. A13 at HK2005629; *see also* Ex. A12.) No contemporaneous documents support this date, except Shanton’s disclosure document. That same document states that “[t]he current implementation of the Distributed Cryptographic Object Method (DCOM) at the application layer is called the Object-Oriented Key Manager (OOKeyMan)." (Ex. A13 at HK2005634.) Similarly, the '702 patent states that the "present invention" is "known as the Distributed Cryptographic Object Model ('DCOM')," and that "[t]he current implementation of the DCOM at the application layer is called the Object-Oriented Key Manager (OOKeyMan)." (Ex. A3 at 5:18–19, 6:40–43.)

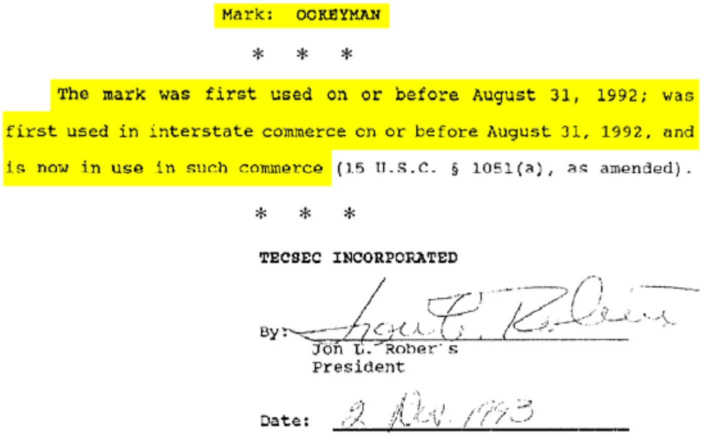
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]



Mark: OOKEYMAN

* * *

The mark was first used on or before August 31, 1992; was first used in interstate commerce on or before August 31, 1992, and is now in use in such commerce (15 U.S.C. § 1051(a), as amended).

* * *

TECSEC INCORPORATED

By:
Jon L. Roberts
President

Date: 2 Nov. 1993

(Ex. A20 at HK0025543–45; *see also* Ex. A21 at 302:15–305:24.)

[redacted]

[redacted]

4. Shanton And His Attorneys Submitted False Declarations Claiming That Shanton Was The Sole Inventor Of The Subject Matter Of The ’702 Patent Family.

Shanton twice signed sworn declarations in connection with the prosecution of the ’702 patent family that he was “***the original, first and sole inventor*** of the subject matter” of the ’702 patent family. (Ex. A7 at IBMTS-00000219–20; Ex. A9 at IBMTS-002635789–90.) There is no genuine dispute that Shanton and his attorneys knew these declarations were false.

[redacted]

[redacted]

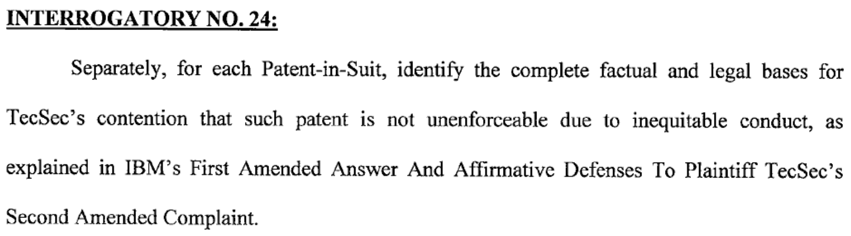
[redacted]

C. Shanton And His Attorneys Intended To Deceive The PTO Into Believing That Shanton Was The Sole Inventor Of The Claimed Subject Matter.

1. Shanton And His Attorneys Knew About Their Copying Of Follendore's Claim, Follendore's Inventorship Claim, And The Prior Existence Of OOKeyMan, And Have No Credible Explanation For Their Failure To Disclose This Highly Material Information.

As discussed above, the evidence indisputably shows that Shanton and his attorneys knew about, but made a deliberate decision not to disclose, their copying of substantial portions of claim 1 of Follendore's '707 patent application into the claims of the '702 patent family, Follendore's inventorship claim and resulting litigation, and the prior existence of the OOKeyMan software Shanton claimed was an embodiment of his invention. TecSec has raised no genuine dispute concerning Shanton's and his attorneys' intent to deceive the PTO—offering no explanation for their failure to disclose this highly material information to the PTO.

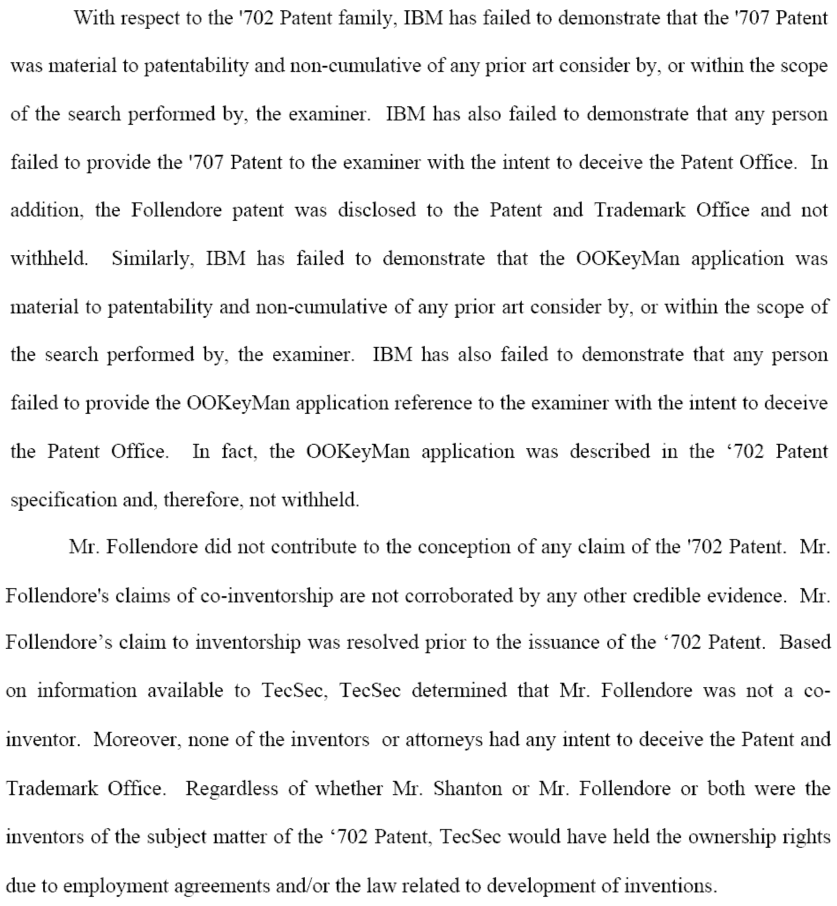
IBM raised each material breach of the duty of candor by Shanton and his attorneys in its amended answer, including: (i) copying substantial portions of claim 1 of Follendore's '707 patent application (D.I. 281 at ¶ 247); (ii) withholding Follendore's inventorship claim (D.I. 281 at ¶¶ 262–265); and (iii) withholding the prior existence of the OOKeyMan application for which Shanton claimed to be an inventor (D.I. 281 at ¶¶ 251–258). IBM thereafter served its Interrogatory No. 24 seeking, for each Patent-in-Suit, "the complete factual and legal bases for TecSec's contention that such patent is not unenforceable due to inequitable conduct":



INTERROGATORY NO. 24:

Separately, for each Patent-in-Suit, identify the complete factual and legal bases for TecSec's contention that such patent is not unenforceable due to inequitable conduct, as explained in IBM's First Amended Answer And Affirmative Defenses To Plaintiff TecSec's Second Amended Complaint.

(Ex. A40 at 9.) Despite its opportunity to explain, TecSec's response (reproduced in its entirety below as it pertains to the '702 patent family), provides only conclusory denials of inequitable conduct with no justification for the repeated failures to disclose the highly material information:



> With respect to the '702 Patent family, IBM has failed to demonstrate that the '707 Patent was material to patentability and non-cumulative of any prior art consider by, or within the scope of the search performed by, the examiner. IBM has also failed to demonstrate that any person failed to provide the '707 Patent to the examiner with the intent to deceive the Patent Office. In addition, the Follendore patent was disclosed to the Patent and Trademark Office and not withheld. Similarly, IBM has failed to demonstrate that the OOKeyMan application was material to patentability and non-cumulative of any prior art consider by, or within the scope of the search performed by, the examiner. IBM has also failed to demonstrate that any person failed to provide the OOKeyMan application reference to the examiner with the intent to deceive the Patent Office. In fact, the OOKeyMan application was described in the '702 Patent specification and, therefore, not withheld.
>
> Mr. Follendore did not contribute to the conception of any claim of the '702 Patent. Mr. Follendore's claims of co-inventorship are not corroborated by any other credible evidence. Mr. Follendore's claim to inventorship was resolved prior to the issuance of the '702 Patent. Based on information available to TecSec, TecSec determined that Mr. Follendore was not a co-inventor. Moreover, none of the inventors or attorneys had any intent to deceive the Patent and Trademark Office. Regardless of whether Mr. Shanton or Mr. Follendore or both were the inventors of the subject matter of the '702 Patent, TecSec would have held the ownership rights due to employment agreements and/or the law related to development of inventions.

(Ex. A40 at 10–11.)

Accordingly, intent to deceive is the ***only*** conclusion supported by the evidence. Moreover, intent should be inferred, because "in the absence of a credible explanation, intent to deceive ***is generally inferred*** from the facts and circumstances surrounding a knowing failure to disclose material information." *Bruno*, 394 F.3d at 1354; *see also Ferring*, 437 F.3d at 1191. The multitude of misrepresentations and omissions described above constitutes "a persistent course of conduct" that was "calculated to obfuscate the threshold issue of inventorship" before the PTO. *PerSeptive Biosystems*, 225 F.3d at 1321.

2. Shanton And His Attorneys Intended To Deceive The PTO And Had A Financial Motive For Doing So.

Even though Shanton and his attorneys knew that Shanton was not the sole inventor of the subject matter claimed in the ’702 patent family (and perhaps not an inventor at all), Shanton signed the disclosure documents and his attorneys submitted them, with an intent to deceive the PTO. “The affirmative act of submitting an affidavit must be construed as being intended to be relied upon.” *Refac,* 81 F.3d at 1583. The only conclusion to be drawn from the submission of the false declarations is that Shanton and his attorneys intended to deceive the PTO into relying on those declarations for determining patentability and inventorship.

[redacted]

[redacted]

[redacted]

[redacted]

In any event, direct proof of their state of mind is not required because intent to deceive or mislead the PTO may be inferred from the mere submission of the false declarations:

> While direct proof of intent to mislead is normally absent, such submissions usually will support the conclusion that the affidavit in which they were contained was the chosen instrument of an intentional scheme to deceive the PTO. ***In any event, proof of the actual state of mind of the applicant or persons associated with or representing an applicant is not required. The intent element … may be proven by a showing of acts the natural consequences of which are presumably intended by the actor.***

Rohm & Haas Co. v. Crystal Chem. Co., 722 F.2d 1556, 1571 (Fed. Cir. 1983) (citation omitted); *see also Paragon Podiatry Lab., Inc. v. KLM Labs., Inc.*, 984 F.2d 1182, 1191 (Fed. Cir. 1993). There is thus no genuine dispute concerning the intent to deceive.

D. Weighing The High Level Of Materiality And The Clear Intent To Deceive The PTO Warrants Summary Judgment Of Unenforceability Of The ’702 Patent Family Due To Inequitable Conduct.

Although a sliding scale is used to weigh materiality and intent, *see Bristol-Myers Squibb Co. v. Rhone-Poulenc Rorer, Inc.*, 326 F.3d 1226, 1234 (Fed. Cir. 2003), IBM has shown by clear and convincing evidence that Shanton and his attorneys failed to disclose highly material information and that they specifically intended to mislead or deceive the examiner. TecSec pointed to no contrary evidence during fact discovery. The undisputed facts thus lead to the inescapable conclusion that Shanton and his attorneys set upon a persistent course of inequitable conduct before the PTO with the express purpose of obfuscating the threshold issue of inventorship. Because TecSec's conduct has been so egregious, the Court should hold each of the patents of the '702 patent family unenforceable. *See Advanced Magnetic*, 607 F.3d at 830, 833 (affirming holding that patent was unenforceable where applicant "concealed the most critical information: he was not the inventor he claimed to be"); *PerSeptive Biosystems*, 225 F.3d at 1320–23 (affirming holding of unenforceability based on at least five specific instances of intentional falsehoods, misrepresentations, and omissions to the PTO, all directed toward the central issue of inventorship); *Frank's Casing*, 293 F.3d at 1376 (affirming holding that patent was unenforceable for failure to name true inventor and deliberate concealment—up to and through litigation—of inventor's relationship and involvement with named inventors); *Paragon*, 984 F.2d at 1190–92 (affirming summary judgment of unenforceability based on materiality of affidavits and inference of intent to deceive based on affirmative acts of submitting misleading affidavits to examiner who had no ability to investigate).

III. Claims 1–12 Of The '433 Patent Are Invalid.

A. The Invention Of The '433 Patent.

U.S. Patent No. 6,694,433 to Kolouch ("the '433 patent") issued on February 17, 2004, from an application filed on October 20, 1999. (Ex. B1.) TecSec contends that the invention of the '433 patent was first conceived in or about April 1999. (Ex. B3 at 7.) April 1999 is thus the critical date for the identification of invalidating prior art.[6]

The '433 patent is directed to "a secure accounting and operational method" to address the situation that "[a]s more businesses adopt electronic systems and interact electronically with

[6] IBM disputes that TecSec can establish a conception date before the filing date, but nonetheless relies upon the April 1999 date for purposes of this motion.

vendors and customers, the ability to reliably audit both controls and transactions is greatly diminished." (Ex. B1 at Abstract, 2:50–53.) The '433 patent attempts to solve this problem by recording input and output data to/from the accounting process as encrypted objects. (*Id.* at Abstract, 2:58–3:1.) "The process of encryption ensures data integrity, as encrypted data that has been modified does not decrypt properly." (*Id.* at 1:42–44.)

The data objects of the '433 patent are formatted with the Extensible Markup Language (XML) which "uses tags to label data objects as to meaning." (*Id.* at 5:13–27.)[7] The '433 patent uses these tags, at least in part, to select a cryptographic scheme for an XML object. (*Id.* at 5:61–67, 6:16–21.) For example, as illustrated in Fig. 7, XML tagged output objects 702 (or objects 704 that are converted to XML objects 705) are provided from the process 700 and 701:

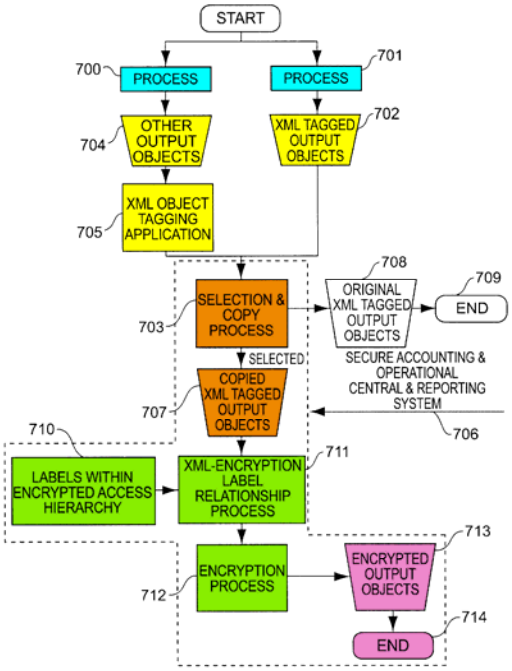
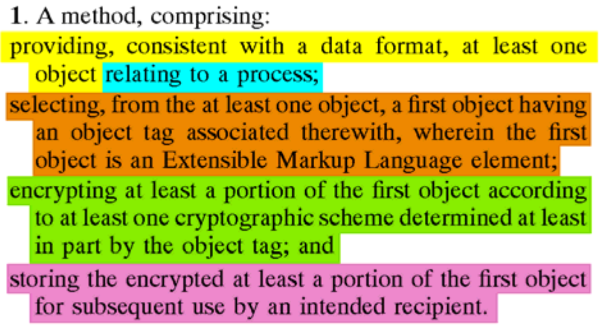

START
700
PROCESS
701
PROCESS
704
OTHER OUTPUT OBJECTS
702
XML TAGGED OUTPUT OBJECTS
705
XML OBJECT TAGGING APPLICATION
708
709
703
SELECTION & COPY PROCESS
ORIGINAL XML TAGGED OUTPUT OBJECTS
END
SELECTED
SECURE ACCOUNTING & OPERATIONAL CENTRAL & REPORTING SYSTEM
707
COPIED XML TAGGED OUTPUT OBJECTS
706
710
711
LABELS WITHIN ENCRYPTED ACCESS HIERARCHY
XML-ENCRYPTION LABEL RELATIONSHIP PROCESS
713
712
ENCRYPTION PROCESS
ENCRYPTED OUTPUT OBJECTS
714
END

FIG. 7



1. A method, comprising:

providing, consistent with a data format, at least one object relating to a process;

selecting, from the at least one object, a first object having an object tag associated therewith, wherein the first object is an Extensible Markup Language element;

encrypting at least a portion of the first object according to at least one cryptographic scheme determined at least in part by the object tag; and

storing the encrypted at least a portion of the first object for subsequent use by an intended recipient.

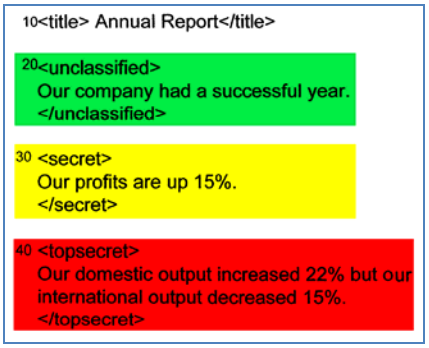
[7] An example of an XML document is illustrated in Fig. 1 of the prior-art Fletcher patent, discussed below. (Ex. B2.)

(Ex. B1 at Fig. 7 and claim 1; *see also id.* at 6:4–9.) The selection and copy process 703 and 707 selects certain XML-tagged output objects 702 and 705 according to control requirements. (*Id.* at 6:4–13.) The system then encrypts 710–712 at least a portion of an output object according to a cryptographic scheme determined at least in part by the object's XML tag. (*Id.* at 5:61–67, 6:16–21.) The encrypted objects are then either passed to, or stored for, appropriate persons, devices, or other systems. (*Id.* at 5:67–6:3, 6:20–24.)

B. U.S. Patent No. 7,010,681 ("Fletcher").

U.S. Patent No. 7,010,681 to Fletcher *et al.* ("Fletcher") was filed on January 29, 1999, before the alleged conception date of the invention of the '433 patent in April 1999. (Ex. B2; Ex. B3 at 7.) Fletcher is thus prior art to the '433 patent under 35 U.S.C. § 102(e).

As in the '433 patent, Fletcher discloses encrypting XML objects using a cryptographic scheme determined at least in part by an XML tag. (*See, e.g.*, Ex. B2 at 3:57–58 (describing "using XML to denote the security requirements of various sections of a document.").) For example, Fletcher discloses that an XML document, such as illustrated in Fig. 1, may have four XML elements—one associated with the document title, and three associated with different levels of security. The first security element 20 (in green) is tagged "<unclassified>," the second security element 30 (in yellow) is tagged "<secret>," and the third security element 40 (in red) is tagged "<topsecret>":



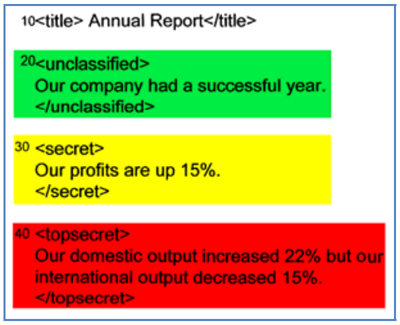
```
10<title> Annual Report</title>

20<unclassified>
  Our company had a successful year.
  </unclassified>

30 <secret>
  Our profits are up 15%.
  </secret>

40 <topsecret>
  Our domestic output increased 22% but our
  international output decreased 15%.
  </topsecret>
```

(*Id.* at Fig. 1; *see also id.* at 3:45–67.)

As illustrated in Fig. 3, Fletcher discloses that the XML document is stored in the "marked-up document DB [database]," and that a user with a "client" device may request the document through "librarian" software running on a computer server. (*Id.* at Fig. 3; *see also id.* at 4:13–22.) Upon a request for the document, the librarian software determines the security level number for each XML security element in the document, based upon the XML tag (e.g., "<unclassified>," "<secret>," or "<topsecret>") and the author's role in the company (e.g., CEO or engineer). (*Id.* at 4:13–37.) For example, the "<secret>" tag for a CEO may be security level 80, whereas the "<secret>" tag for an engineer may be security level 50. (*Id.* at 4:38–47.) These security level numbers in turn determine the cryptographic scheme, such as: (i) no encryption for security levels 0–9; (ii) 56-bit DES for security levels 10–49; (iii) 128-bit DES for security levels 50–75; and (iv) 256-bit DES for security levels 76–99. (*Id.* at 5:13–20, Fig. 4.)

The librarian software then selects each XML security element from the XML document to which the requester is permitted access, and filters out the others. (*Id.* at 5:52–65.) For example, if the requester is permitted access to "secret" information, but not "topsecret" information, the librarian creates a filtered document by removing the "topsecret" XML security element, so that the XML document of Fig. 1 would be filtered as follows:

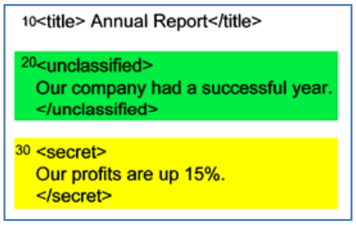
Original XML Document



```
10<title> Annual Report</title>

20<unclassified>
  Our company had a successful year.
  </unclassified>

30 <secret>
  Our profits are up 15%.
  </secret>

40 <topsecret>
  Our domestic output increased 22% but our
  international output decreased 15%.
  </topsecret>
```

→

Filtered XML Document



```
10<title> Annual Report</title>

20<unclassified>
  Our company had a successful year.
  </unclassified>

30 <secret>
  Our profits are up 15%.
  </secret>
```

(*Id.* at 5:52–65, Fig. 1.) The librarian software then selects the cryptographic scheme based upon the most secure portion of the filtered document ("<secret>" in this example) and encrypts the XML document. (*Id.* at 6:10–15, 34–35; *see also id.* at 6:15–30.) For example, if the author is the CEO, the "<secret>" tag requires security level 80, which uses 256-bit DES. Alternatively, if the author is an engineer, the "<secret>" tag requires security level 50, which uses 128-bit DES. (*Id.* at 4:38–47, Fig. 4.) The cryptographic scheme is thus determined at least in part based upon the object tag of the most secure XML element in the filtered XML document, e.g., the "<secret>" object tag. (*Id.*; *see also id.* at 6:10–30.) As a result of the process, rather than encrypting the entire original XML document, only a portion of the original XML document is encrypted according to the selected cryptographic scheme. (*See, e.g., id.* at 6:10–35.)

C. Claims 1–8 And 10–11 Of The '433 Patent Are Anticipated By Fletcher.

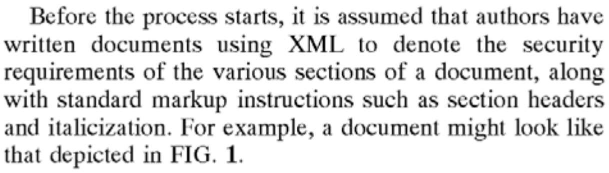
As set forth in the claim chart attached hereto as Ex. B4, and confirmed by the supporting declaration of IBM's computer security expert Paul Clark, D.Sc., filed concurrently herewith ("Clark Decl."), there is no genuine issue of material fact that Fletcher discloses every limitation of claims 1–8 and 10–11 of the '433 patent. Significantly, IBM provided a detailed invalidity claim chart during the course of discovery demonstrating anticipation of the '433 patent by Fletcher. (Ex. B6.) In response to IBM's Interrogatory No. 15 seeking that TecSec "explain in detail for each such claim element the complete factual and legal basis for why TecSec contends it is not disclosed," TecSec provided no explanation whatsoever for ***any*** of the claim elements. (Ex. B7 at 9–11.) Moreover, after the close of discovery, TecSec's expert Stuart G. Stubblebine, Ph.D., asserted that Fletcher does not disclose all of the limitations of the '433 patent claims. (Ex. B8 at 85–89.) But as discussed below, Dr. Stubblebine's assertions are conclusory and not tied to the actual limitations of the '433 patent claims. These conclusory and irrelevant assertions cannot raise a genuine issue of fact for trial. *See Sitrick*, 516 F.3d at 1001

("Conclusory expert assertions cannot raise triable issues of material fact on summary judgment."). Claims 1–8 and 10–11 of the '433 patent are thus invalid under 35 U.S.C. § 102(e). *See Celeritas Techs., Ltd. v. Rockwell Int'l Corp.*, 150 F.3d 1354, 1361 (Fed. Cir. 1998) ("It is well settled that a claim is anticipated if each and every limitation is found either expressly or inherently in a single prior art reference.").

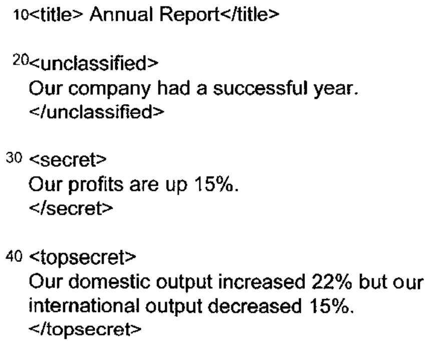
1. Fletcher Discloses Every Element Of Claim 1.

(a): "providing, consistent with a data format, at least one object relating to a process"

Fletcher discloses providing, consistent with the XML data format, at least one object consisting of a written document relating to a process, such as shown in Fig. 1:



Before the process starts, it is assumed that authors have written documents using XML to denote the security requirements of the various sections of a document, along with standard markup instructions such as section headers and italicization. For example, a document might look like that depicted in FIG. 1.



```
10<title> Annual Report</title>

20<unclassified>
  Our company had a successful year.
  </unclassified>

30 <secret>
  Our profits are up 15%.
  </secret>

40 <topsecret>
  Our domestic output increased 22% but our
  international output decreased 15%.
  </topsecret>
```

(Ex. B2 at 3:56–61, Fig. 1; *see also id.* at 5:53–55 ("The librarian uses the document name to fetch the entire document from the document database."); Clark Decl. ¶¶ 9-10.) TecSec's expert, Dr. Stubblebine, does not dispute that Fletcher discloses this element. (Ex. B8 at 86–88.)

(b): "selecting, from the at least one object, a first object having an object tag associated therewith, wherein the first object is an Extensible Markup Language element"

Fletcher discloses selecting from the XML document (e.g., the at least one object) a first object consisting of an Extensible Markup Language (XML) element having an object tag associated therewith. Specifically, when a user requests a document, the librarian software shown in Fig. 3 selects each tagged element in the XML document that the user is permitted to access to create a filtered XML document. For example, the librarian software parses each object tag in the XML document, such as the "<unclassified>," "<secret>," and "<topsecret>" tagged elements of Fig. 1, to determine if the user is authorized to see this level of information. Only those XML elements that the user is authorized to access are selected for encryption, and the rest are filtered out of the document. (Ex. B2 at 5:52–65; Clark Decl. at ¶ 12.) The remaining XML elements are encrypted.

TecSec's expert contends that Fletcher does not disclose the "selecting" step because, according to Dr. Stubblebine, "[i]n the '681 patent, those objects with a security tag may be selected for *removal*." (Ex. B8 at 87 (emphasis in original).) But this is a distinction without a difference. As discussed above, Fletcher describes starting with an entire XML document, parsing ***each*** tag in the document to determine if the user is authorized to see that information, and removing those XML objects that the user is not authorized to access. (Ex. B2 at 5:52–65; Clark Decl. at ¶ 12.) The parsing process thus clearly selects which XML objects are removed from the document, and also which XML objects are ***not*** removed from the document. In this way, the parsing process selects which XML objects to encrypt (e.g., the "<unclassified>" and "<secret>" objects in the example above). (Ex. B2 at 5:58–60 ("It parses ***each tag*** in the text and again uses the author's role to determine the absolute security level of the section governed by the tag. If the user is not authorized to see this level of information, the section is removed from this temporary copy of the document.").) Dr. Stubblebine's assertion to the contrary has no basis in fact and must be rejected.

(c): "encrypting at least a portion of the first object according to at least one cryptographic scheme determined at least in part by the object tag"

Fletcher discloses encrypting at least a portion of the first object (e.g., the "secret" XML object tag in the example above) according to at least one cryptographic scheme determined at least in part by the object tag. For example, as set forth above, the XML document may have three XML elements as illustrated in Fig. 1, tagged as "<unclassified>," "<secret>," and "<topsecret>." (Ex. B2 at Fig. 1; Clark Decl. ¶ 15.) Fletcher discloses that the author's role (e.g., CEO or engineer) plus the object tag (e.g., topsecret, secret, or classified) determine a security level number. (Ex. B2 at 4:38–47; Clark Decl. ¶ 16.) These security level numbers in turn determine the cryptographic scheme, such as 56-bit DES for security levels 10–49, 128-bit DES for security levels 50–75, and 256-bit DES for security levels 76–99. (Ex. B2 at 5:13–20, Fig. 4; Clark Decl. ¶ 17.) The librarian software selects the cryptographic scheme necessary to meet the security requirement for the most secure XML element of the filtered XML document (e.g., the "secret" XML object in the example above) and encrypts each XML element using the selected cryptographic scheme. (Ex. B2 at 6:10–15, 34–35; Clark Decl. ¶ 18.) The cryptographic scheme for the first object (e.g., the "secret" XML object in the example above) is thus determined at least in part based upon the object tag. (Ex. B2 at 6:15–30; Clark Decl. ¶ 19.) TecSec's expert does not dispute that Fletcher discloses this element. (Ex. B8 at 86–88.)[8]

(d): "storing the encrypted at least a portion of the first object for subsequent use by an intended recipient"

[8] Dr. Stubblebine instead raises other alleged "differences" from the '433 patent, namely that "the '681 patent does not teach or suggest object-level encryption operating on sub-file objects" and "does not provide for the capability of different encryption algorithms applied in the same document." (Ex. B8 at 87–88.) But these are not limitations of the asserted claims, and thus such alleged "differences" are entirely irrelevant. Indeed, all of the claims of the '433 patent recite either encrypting "at least a portion" of the XML document, not ***only*** a portion (*see, e.g.*, claims 1 and 7 (Ex. B1 at 7:1–3, 8:22–24)), or encrypting "at least one of the plurality of objects" of the XML document, not ***only*** one of the objects (*see, e.g.*, claim 10 (*id.* at 8:47–51)).

Fletcher discloses that the encrypted portion of the first object may be stored for subsequent use by an intended recipient. (Ex. B2 at 1:22–26; Clark Decl. ¶ 21.) TecSec's expert does not dispute that Fletcher discloses this element. (Ex. B8 at 86–88.)

2. Fletcher Discloses Every Element Of Claims 2–8 And 10–11.

Claims 2–8 and 10–11 of the '433 patent are substantially the same as claim 1 and are invalid for the reasons set forth above. For example, similar to claim 1, there is no genuine dispute that Fletcher discloses each of the elements of claims 2–8 and 10–11 of the '433 patent, as set forth in the claim chart of Ex. B4. (Clark Decl. ¶¶ 23-54.) TecSec's expert provides no basis for concluding otherwise. (Ex. B8 at 86–89.) These claims are thus invalid as anticipated.

D. Claims 9 and 12 Are Invalid For Failure To Comply With The Written Description Requirement Of 35 U.S.C. § 112.

There is no genuine dispute that the '433 patent specification lacks any written description for the limitations of claims 9 and 12. For example, both claims require "***another*** Extensible Markup Language." (Ex. B1 at 8:34–35, 8:58–59.) But nothing in the '433 patent application, as filed, disclosed or suggested more than one Extensible Markup Language. (Ex. B5.) To the contrary, the '433 patent specification refers to "***the*** Extensible Markup Language," *i.e.*, only one such language. (Ex. B1 at 5:14–16.)

Significantly, IBM expressly identified this limitation during the discovery period as part of its invalidity contentions as lacking written description support in the specification. (Ex. B6 at 25.) And in response to IBM's Interrogatory No. 16 seeking TecSec's complete bases (if any) for any disagreement with IBM's invalidity contentions, TecSec was unable to identify ***anything*** in the '433 patent specification that allegedly discloses this limitation. (Ex. B7 at 29.) There is thus no genuine dispute of material fact and claims 9 and 12 should be held invalid for failure to comply with the written description requirement of 35 U.S.C. § 112 ¶ 1. *See ICU Med.*, 558

F.3d at 1379 (affirming grant of summary judgment for failure to comply with the written description requirement because the patentee "has failed to point to any disclosure in the patent specification that describes a spikeless valve with a preslit trampoline seal" as claimed); *TurboCare Div. of Demag Delaval Turbomachinery Corp. v. Gen. Elec. Co.*, 264 F.3d 1111, 1119 (Fed. Cir. 2001) (affirming grant of summary judgment for failure to comply with the written description requirement because the "original disclosure is completely lacking in any description of an embodiment in which the spring is located between the casing shoulders and the inner surface of the outer ring portion of the ring segment" as claimed.).

IV. Claims 1–18 Of The '448 Patent Are Invalid.

A. The Invention Of The '448 Patent.

U.S. Patent No. 7,069,448 to Odell *et al*. ("the '448 patent") issued on June 27, 2006, from an application filed on December 5, 2002. (Ex. C1.) The '448 patent claims priority to U.S. Provisional Application No. 60/337,530, filed on December 5, 2001. (*Id*.) TecSec contends that the subject matter of the '448 patent was invented in or about September 2001. (Ex. B3 at 7.) September 2001 is thus the critical date for the identification of invalidating prior art.[9]

The '448 patent is directed to "context-oriented cryptographic processing in a parallel processing environment." (Ex. C1 at 1:38–40.) The '448 patent acknowledges that parallel cryptographic processing systems were known in the prior art. (*Id*. at 1:65–67.) The patent asserts, however, that "there remains a need for an efficient manner of effectuating cryptographic processing in a parallel processing environment." (*Id*. at 2:1–3.) To that end, the '448 patent

[9] IBM disputes that TecSec can establish a conception date before the provisional application filing date, but nonetheless relies upon the September 2001 date for purposes of this motion.

describes and claims a specific architecture for cryptographic processing of input data in a parallel processing environment to increase the speed of the encryption or decryption process.

As reflected in Fig. 1 and claim 1, the ’448 patent discloses a system and method that extracts “control data” and “main data” from “input data,” such that control and cryptographic “parameters” based upon the “control data” are used to control the distribution of the main data to each of a number of different processors for encryption or decryption. The data output from each processor is then recombined to provide the “output data”:

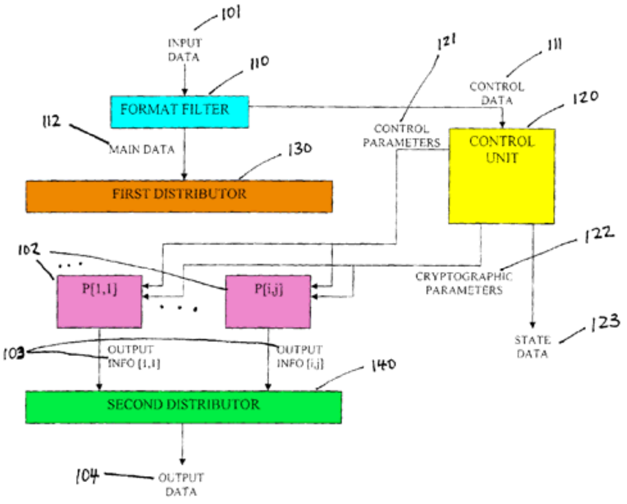
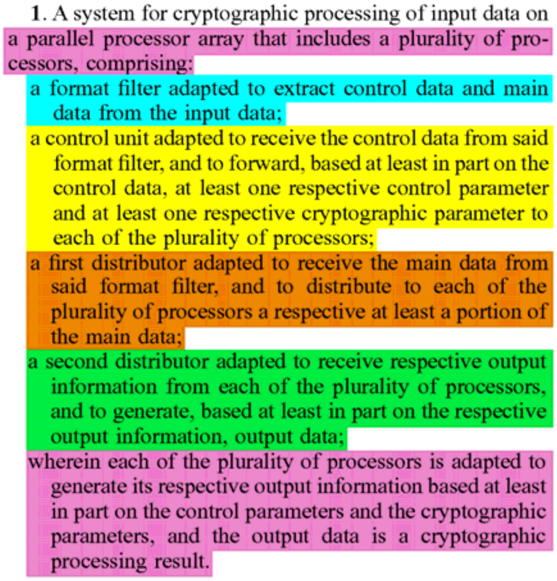


FIGURE 1


1. A system for cryptographic processing of input data on a parallel processor array that includes a plurality of processors, comprising:

a format filter adapted to extract control data and main data from the input data;

a control unit adapted to receive the control data from said format filter, and to forward, based at least in part on the control data, at least one respective control parameter and at least one respective cryptographic parameter to each of the plurality of processors;

a first distributor adapted to receive the main data from said format filter, and to distribute to each of the plurality of processors a respective at least a portion of the main data;

a second distributor adapted to receive respective output information from each of the plurality of processors, and to generate, based at least in part on the respective output information, output data;

wherein each of the plurality of processors is adapted to generate its respective output information based at least in part on the control parameters and the cryptographic parameters, and the output data is a cryptographic processing result.

(*Id*. at 2:20–42, 3:48–4:52, Fig. 1, claim 1.) For example, “input data” 101 is received by a “format filter” 110 that extracts “control data” 111 and “main data” 112, and sends the “control data” 111 to a “control unit” 120 and the “main data” 112 to a “first distributor” 130. (*Id.*) Based on the “control data” 111, the “control unit” 120 directs the “first distributor” 130 to distribute portions of the “main data” 112 to each of the multiple “processors” 102 in the “array” to be cryptographically processed in “parallel” according to “control parameters” 121 and “cryptographic parameters” 122 forwarded by the “control unit” 120. (*Id.*) The encrypted or decrypted portions of “main data” 112 processed by each of the “processors” 102, referred to as "output information" 103, are then sent to a "second distributor" 140. (*Id.*) The "second distributor" 140 then generates "output data" 104 based on the "output information" 103 from each of the "processors" 102. (*Id.*)

B. U.S. Patent No. 7,600,131 ("Krishna").

U.S. Patent No. 7,600,131 to Krishna *et al*. ("Krishna") was filed on July 6, 2000, before the alleged conception date of the invention of the '448 patent in September 2001. (Ex. C2; Ex. B3 at 7.) Krishna is thus prior art to the '448 patent under 35 U.S.C. § 102(e).

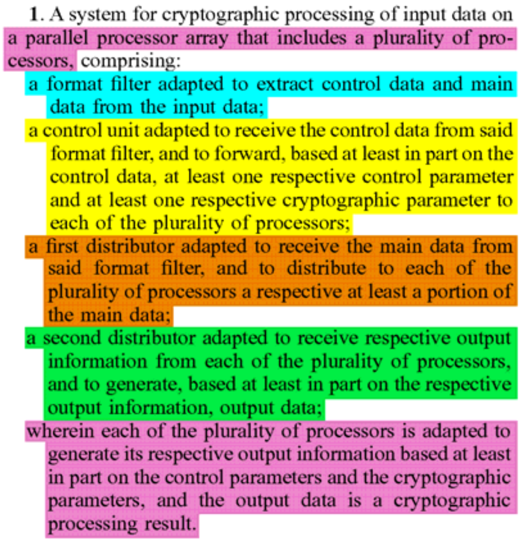
Krishna describes "an architecture for a cryptography accelerator chip that allows significant performance improvements over previous prior art designs." (Ex. C2 at 2:12–14.) "[T]he architecture enables parallel processing of packets through a plurality of cryptography engines and includes a classification engine configured to efficiently process encryption/decryption of data packets." (*Id*. at 2:15–18.) To that end, Krishna describes a parallel cryptographic processing architecture, as reflected in Figure 3. (*Id*. at Fig. 3.) In this architecture, "IP packets" are read by an "Input FIFO" 302, which sends "packet header information" to a "packet classifier" 304 and "packet data" to a "packet distributor" 306. (*Id*. at 7:60–8:42.) Upon receiving the "packet header information," a classification engine in the "packet classifier" 304 determines "security association information" required for processing the packet, such as "encryption keys, data, etc." (*Id.*) The "security association information" determined by the "packet classifier" 304 is sent to the "packet distributor" 306, which distributes the "security association information" and the "packet data" among a "plurality of cryptography engines" 316. (*Id.*) Processed "packet cells" are reassembled into "packets" and sent off the chip by an "output FIFO" 318. (*Id.*)

C. Claims 1–18 Of The ’448 Patent Are Anticipated By Krishna.

As set forth in the claim chart attached hereto as Ex. C3, and confirmed by the supporting declaration of IBM’s cryptography expert Matthew Blaze, Ph.D., filed concurrently herewith (“Blaze Decl.”), and the deposition testimony of TecSec’s cryptography expert Aviel D. Rubin, Ph.D. (Ex. C5), there is no genuine issue of material fact that Krishna discloses every limitation of claims 1–18 of the ’448 patent. Significantly, IBM provided a detailed invalidity claim chart during the course of discovery demonstrating anticipation of the ’448 patent by Krishna. (Ex. B6.) In response to IBM’s Interrogatory No. 15 seeking that TecSec “explain in detail for each such claim element the complete factual and legal basis for why TecSec contends it is not disclosed,” TecSec provided no explanation whatsoever for ***any*** of the claim elements. (Ex. B7 at 1, 11–13.) Moreover, after the close of discovery, TecSec’s expert Dr. Rubin asserted in his rebuttal expert report that Krishna does not disclose all of the limitations of the ’448 patent claims. (Ex. C4 at ¶¶ 55–70.) But Dr. Rubin’s assertions are conclusory and impermissibly contradict the plain language of the claims, and the positions Dr. Rubin himself took in asserting infringement of those same claims by IBM. These conclusory and contradictory assertions cannot raise a genuine issue of fact for trial. *See Sitrick*, 516 F.3d at 1001 (“Conclusory expert assertions cannot raise triable issues of material fact on summary judgment.”). Furthermore, during his deposition, Dr. Rubin retreated from the opinions set forth in his rebuttal report with regard to any purported distinctions between Krishna and the ’448 patent. (Ex. C5.) Claims 1–18 of the ’448 patent are thus invalid under 35 U.S.C. § 102(e). *See Celeritas*, 150 F.3d at 1361.

1. Krishna Discloses Every Element Of Claim 1.

There is no genuine dispute that Krishna discloses every element of claim 1 of the ’448 patent, as illustrated by the following color-coded claim 1 and Fig. 3 of Krishna:



1. A system for cryptographic processing of input data on a parallel processor array that includes a plurality of processors, comprising:

a format filter adapted to extract control data and main data from the input data;

a control unit adapted to receive the control data from said format filter, and to forward, based at least in part on the control data, at least one respective control parameter and at least one respective cryptographic parameter to each of the plurality of processors;

a first distributor adapted to receive the main data from said format filter, and to distribute to each of the plurality of processors a respective at least a portion of the main data;

a second distributor adapted to receive respective output information from each of the plurality of processors, and to generate, based at least in part on the respective output information, output data;

wherein each of the plurality of processors is adapted to generate its respective output information based at least in part on the control parameters and the cryptographic parameters, and the output data is a cryptographic processing result.

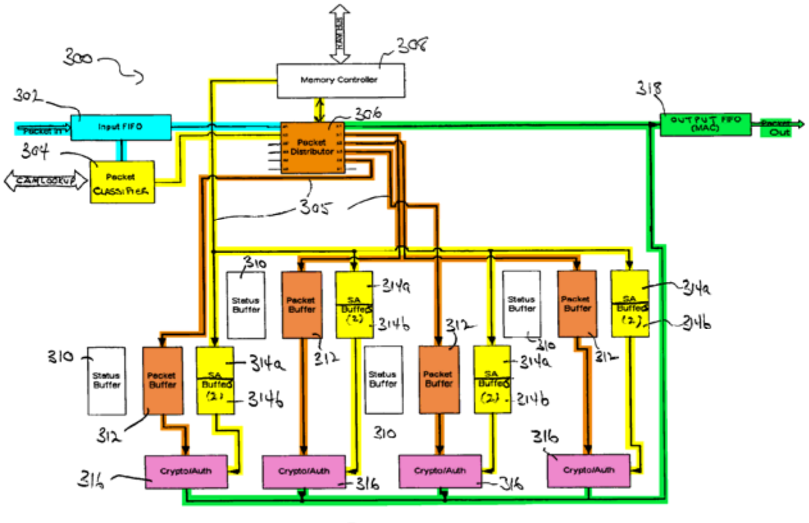


FIG. 3

(Ex. C1 at claim 1; Ex. C2 at Fig. 3.) The limitations of claim 1 are discussed below. (*See also* Ex. C3.)

(a): "a system for cryptographic processing of input data on a parallel processor array that includes a plurality of processors"

As illustrated in Fig. 3, Krishna discloses a system 300 for cryptographic processing of "input data" received in Input FIFO 302 on a "parallel processor array" that includes a "plurality of processors" (cryptographic processing engines 316):

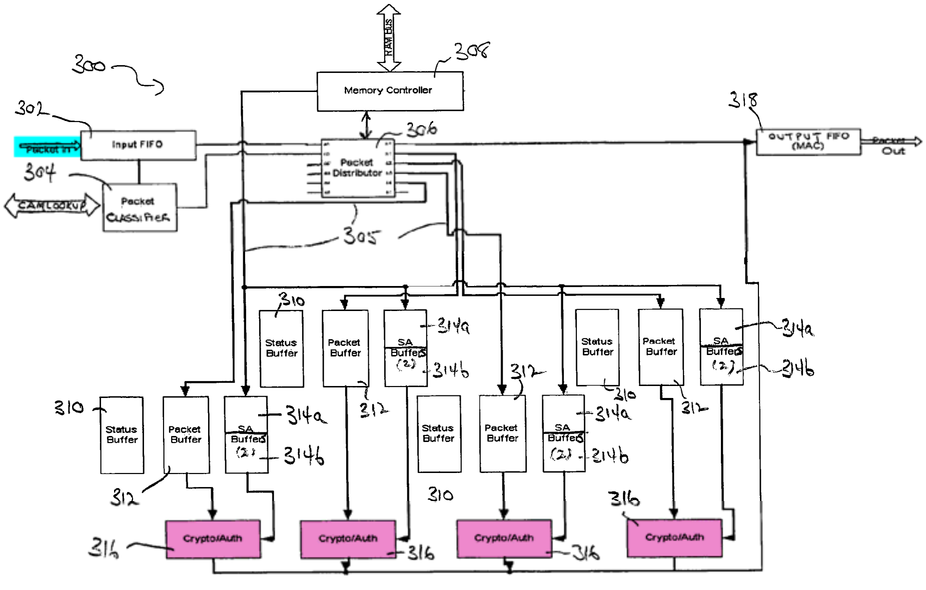
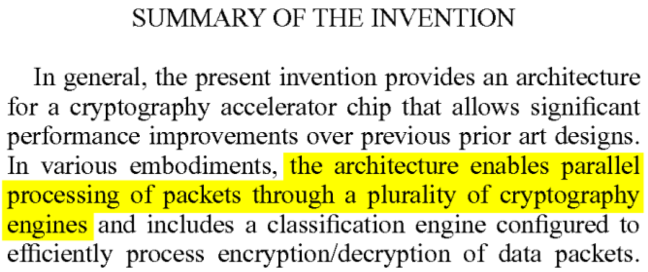


FIG. 3

(Ex. C2 at Fig. 3; *see also id.* at Fig. 2 with input FIFO 202 and cryptographic processing engines 214; *id.* at 3:66–4:3; Blaze Decl. ¶ 9.) Krishna explains that this architecture enables parallel processing of packets ("input data") through a "plurality of processors" referred to as "cryptography engines" or "cryptographic processing engines":



SUMMARY OF THE INVENTION

In general, the present invention provides an architecture for a cryptography accelerator chip that allows significant performance improvements over previous prior art designs. In various embodiments, the architecture enables parallel processing of packets through a plurality of cryptography engines and includes a classification engine configured to efficiently process encryption/decryption of data packets.

(Ex. C2 at 2:10–18; *see also id.* at Abstract ("[T]he architecture enables parallel processing of packets through a plurality of cryptography engines."); *id.* at 2:51–53; Blaze Decl. ¶ 10.). Krishna also describes an implementation of the architecture for "cell-based" processing, where IP packets are split into "fixed-sized cells," which are processed and then "reassembled (recombined) into packets." (Ex. C2 at 3:47–56; Blaze Decl. ¶ 11.) Notably, TecSec's expert agrees that Krishna describes a "parallel processor array that includes a plurality of processors." (Ex. C5 at 231:20–232:2.)

(b): "a format filter adapted to extract control data and main data from the input data"

As illustrated in Fig. 3, Krishna discloses a "format filter" (Input FIFO 302) adapted to extract "control data" (packet header information) and "main data" (packet data) from the "input data" (input IP packets). The "control data" is sent to the packet classifier 304, and the "main data" is sent to the packet distributor 306:

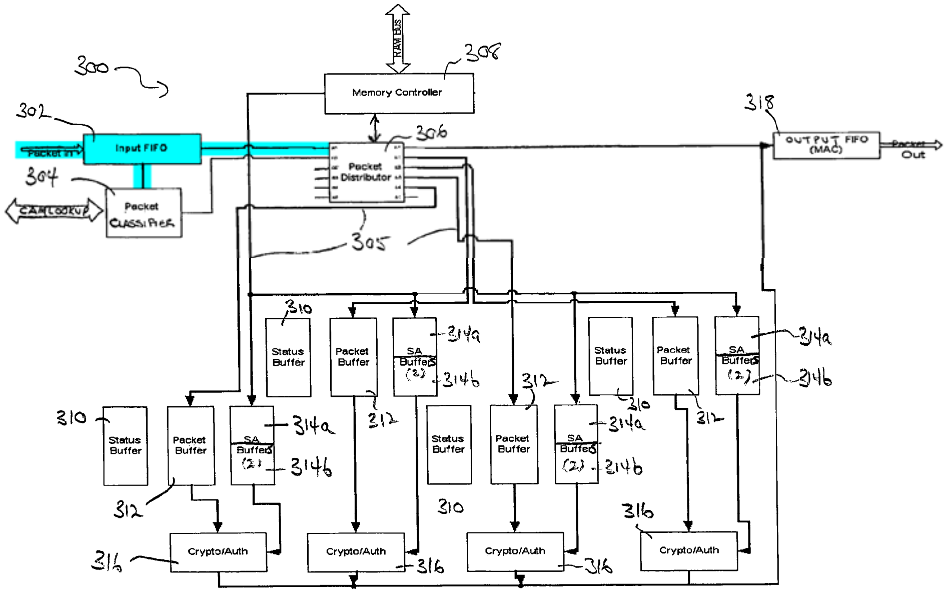
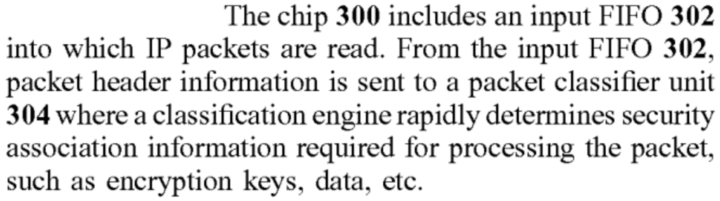


FIG. 3

(Ex. C2 at Fig. 3; *see also id.* at Fig. 2; Blaze Decl. ¶ 13.) For example, Krishna explains that once the input IP packets are read into the "format filter" (Input FIFO 302), "packet header information is sent to a packet classifier unit 304 where a classification engine rapidly determines security association information required for processing the packet, such as encryption keys, data, etc.":



The chip **300** includes an input FIFO **302** into which IP packets are read. From the input FIFO **302**, packet header information is sent to a packet classifier unit **304** where a classification engine rapidly determines security association information required for processing the packet, such as encryption keys, data, etc.

(Ex. C2 at 7:62–67; *see also id.* at 5:54–57, Figs. 2–3; Blaze Decl. ¶ 14.)

In his rebuttal report, Dr. Rubin denied that Krishna discloses the claimed "format filter," but provided no support for his denial, stating without explanation that "[b]ased on the teachings of Krishna '131, the input FIFO does not perform the claimed functionality." (Ex. C4 at ¶ 58.) Such a conclusory assertion, which is at odds with the plain disclosure of Krishna, does not raise a genuine issue of material fact for trial. *See Sitrick*, 516 F.3d at 1001. Moreover, Dr. Rubin admitted at his deposition that IP packets constitute “input data” and that Krishna’s Input FIFO 302 sends packet header information, comprising “control data,” to the packet classifier 304 and packet data, comprising “main data,” to the packet distributor 306. (Ex. C5 at 232:14–233:11, 233:18–235:6.)

> ***(c): “a control unit adapted to receive the control data from said format filter, and to forward, based at least in part on the control data, at least one respective control parameter and at least one respective cryptographic parameter to each of the plurality of processors”***

As illustrated in Fig. 3, Krishna discloses a “control unit” (packet classifier 304) that receives “control data” (packet header information) from the “format filter” (Input FIFO 302):

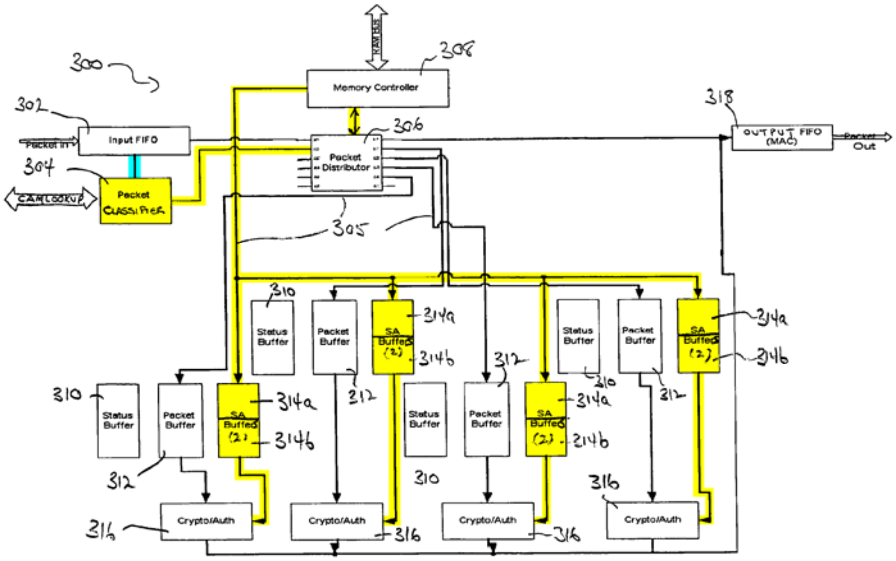


FIG. 3

(Ex. C2 at Fig. 3; *see also id.* at Fig. 2; 8:10–36; 6:1–10; Blaze Decl. ¶ 16.) As illustrated, the “control unit” (packet classifier 304) forwards, based at least in part on the “control data” (packet header information), security association information to each of the plurality of cryptographic processing engines 316 (through packet distributor 306, memory controller 308, and security association information (SA) buffers 314a and b). This security association information includes at least one respective “control parameter” (e.g., “u32 byteCount,” which identifies the “[t]otal payload bytes processed via this entry") and at least one respective "cryptographic parameter" (e.g., "cryptoState algoCrypto," which identifies "[k]eys and other parameters for crypto," or "u8 crypto:2," which identifies the type of encryption or decryption, such as "DES, 3DES, RC4, NONE"). (Ex. C2 at 14:1–35; Ex. C5 at 235:7–236:15; Blaze Decl. ¶¶ 16–19.)

For example, based upon the "control data" (packet header information), the "control unit" (packet classifier 304) determines the "security association information required to process the packet, such as encryption keys, data, etc." (Ex. C2 at 7:63–67; *see also id*. at 5:54–57; Ex. C5 at 235:7–236:10, 244:23–245:6; Blaze Decl. ¶ 18.) The "control unit" (packet classifier 304) forwards this information to the cryptographic processing engines 316 based at least in part on the "control data" (packet header information). (Ex. C2 at 12:60–66; *see also id*. at 13:37–43; Ex. C5 at 236:11–15; Blaze Decl. ¶ 19.) Krishna explains that this security association information is sent to packet distributor 306 for distribution to each of the "plurality of processors" (cryptographic processing engines 316). (Ex. C2 at 7:63–67, 8:10–17; *see also id*. at 6:1–9; Ex. C5 at 236:11–15; Blaze Decl. ¶ 19.)

In his rebuttal report, TecSec's expert denied that Krishna discloses the claimed "control unit" because, in his opinion: (1) the security association information is sent from the memory controller 308 rather than the packet classifier 304; and (2) the security association information is sent to the plurality of cryptographic processing engines via the packet distributor 306:

> According to Krishna '131, packet classifier unit 304 sends security association information to packet distributor 306, not to each of the plurality of processors. Moreover, packet classifier unit 304, as described by Krishna '131, does not send a control parameter and a cryptographic parameter to each of the plurality of processors. Rather, security association information is sent from memory controller 308.

(Ex. C4 at ¶ 59.) This is both factually incorrect and irrelevant, as Dr. Rubin himself acknowledged at his deposition. First, Krishna expressly states that the security association information is determined by, and sent from, the packet classifier unit, not the memory controller. (Ex. C2 at 8:10–12 ("The security association information ***determined by the packet classifier unit 304*** is sent to a packet distributor unit 306.").) Dr. Rubin admitted at his deposition that this purported distinction was invalid, and that the security association information ***is*** sent form the packet classifier unit to the plurality of cryptographic processing engines. (Ex. C5 at 224:5–11, 238:14-239:16.)[10] Second, the fact that the packet classifier sends security association information to the plurality of cryptography engines via the packet distributor and memory controller is irrelevant. Nothing in the '448 patent claims requires that the "control unit" must forward the parameters to the "plurality of processors" directly. (Ex. C1.) Indeed, Dr. Rubin admitted during his deposition that Krishna's description of sending security association information ("control parameters" and "cryptographic parameters") to the plurality of cryptographic engines 316 ("plurality of processors") via the packet distributor 306 ("first distributor") meets the limitations of the asserted claims. (C5 at 226:18–227:16.) Under these circumstances, there is no genuine issue of material fact. *See Sitrick*, 516 F.3d at 1001.

(d): "a first distributor adapted to receive the main data from said format filter, and to distribute to each of the plurality of processors a respective at least a portion of the main data"

As illustrated in Fig. 3, Krishna discloses a "first distributor" (packet distributor 306) adapted to receive the "main data" (packet data) from the "format filter" (Input FIFO 302), and to distribute (through packet buffers 312) to each of the "plurality of processors" (cryptographic processing engines 316) a respective at least a portion of the "main data":

[10] In any event, according to Krishna, the memory controller is an optional component that is "unnecessary" in embodiments where "the memory is connected directly with the cryptography engines 316 and packet classifier 304." (Ex. C2 at 8:5-9.)

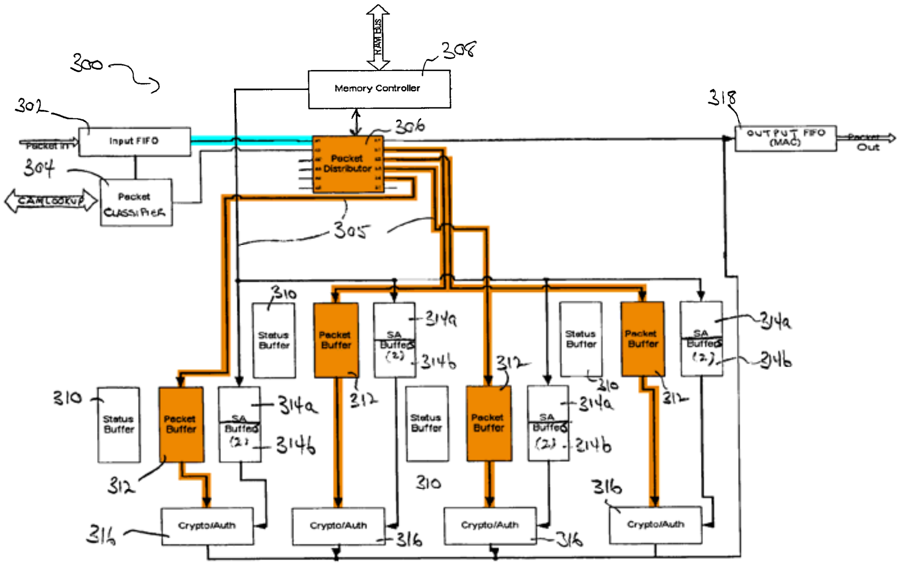


FIG. 3

(Ex. C2 at Fig. 3; Blaze Decl. ¶ 21.) For example, Krishna explains that the “first distributor” (packet distributor 306) distributes the “main data” (packet data) via the internal bus 305 among the “plurality of processors” (plurality of cryptography processing engines 316). (Ex. C2 at 8:13–17; *see also id.* at 6:4–9; Blaze Dec. ¶ 22.)

In his expert report, Dr. Rubin denied that Krishna discloses the claimed “first distributor” because he claimed that: (i) “the packet distributor 206 of Krishna ‘131 is not ‘adapted to receive the main data from said format filter’”; and (ii) “Krishna ‘131 fails to disclose a first distributor that distributes ‘to each of the plurality of processors a respective at least a portion of the main data.’” (Ex. C4 at ¶ 60.) These conclusory assertions, however, directly contradict the express disclosure of Krishna, as Dr. Rubin admitted during his deposition. For example, as illustrated by Fig. 3, the ***only*** pathway from the “format filter” (Input FIFO 302) to the “plurality of processors” (plurality of cryptographic processing engines 316) is through the “first distributor” (packet distributor 306). Clearly, therefore, the packet distributor 306 receives the “main data” (packet data) from the “format filter” (Input FIFO 306). (Ex. C2 at 8:13–17 (“The packet distributor unit 306 then distributes ... the packet data via the internal bus 305 among a plurality of cryptography processing engines 316.").) Dr. Rubin admitted at his deposition that the Input FIFO 306 extracts "main data" and "control data" form the "input data" (IP packets). (Ex. C5 at 232:14–233:11, 233:18–235:6.) Krishna also expressly discloses that the packet distributor 306 distributes "main data" to each of the cryptographic processing engines 316. (Ex. C2 at 8:13–17; *see also id.* at 2:51–53 ("The data packets are cryptographically processed in parallel on the cryptographic processing engines."); *id.* at 6:24–26 ("The distributor 206 selects the next free engine in round-robin fashion within a given flow.").) Dr. Rubin admitted at his deposition that the fact that the packet distributor distributes portions of "main data" to the "plurality of processors" in a round-robin fashion does not take Krishna out of the scope of the '448 patent claims. (Ex. C5 at 239:23–241:4.)

(e): "a second distributor adapted to receive respective output information from each of the plurality of processors, and to generate, based at least in part on the respective output information, output data"

As illustrated in Fig. 3, Krishna discloses a "second distributor" (output FIFO 318 under control of packet distributor 306) adapted to receive respective "output information" from each of the "plurality of processors" (cryptographic processing engines 316), and to generate "output data" (packet out) based in part on the respective "output information":

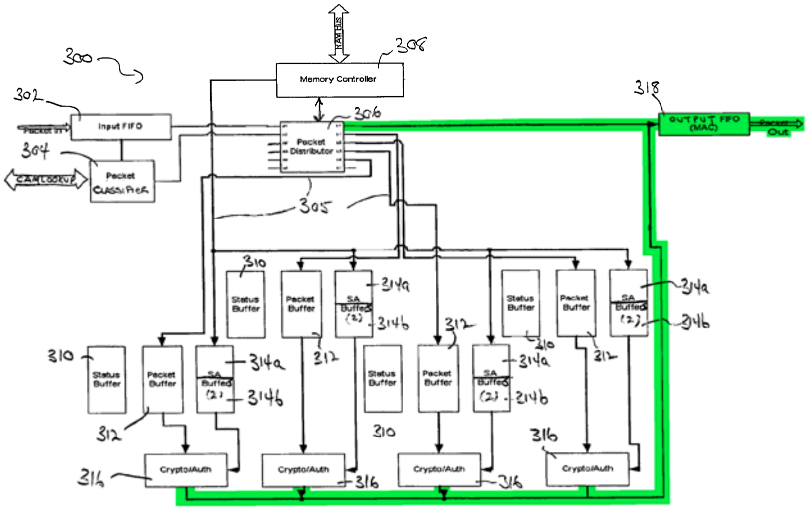


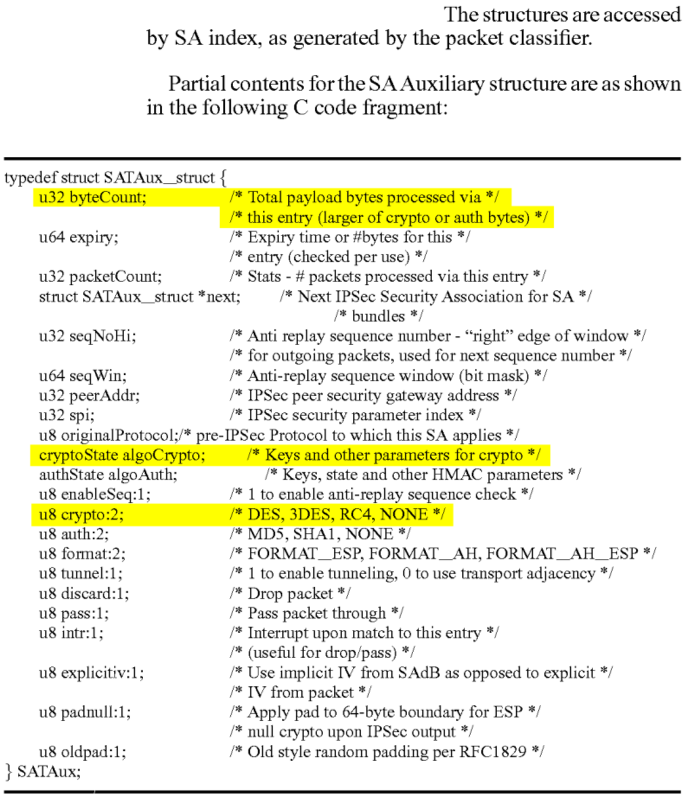
FIG. 3

(Ex. C2 at Fig. 3; Blaze Decl. ¶ 24.) Krishna explains that the output FIFO 318, under control of packet distributor 306, reassembles the packet cells from each of the cryptographic processing engines 316 into packets ("output information") and then outputs those packets from the chip. (Ex. C2 at 8:39–42; *see also id*. at 3:52–56; 7:56–59; Blaze Decl. ¶ 25.)

In his expert report, TecSec's expert Dr. Rubin denied that Krishna discloses the claimed "second distributor," but provided no support for his denial, stating without explanation that "[t]he FIFO 318 of Krishna '131 does not receive respective output information from each of the plurality of processor" or "generate respective output data, based at least in part on the respective output information." (Ex. C4 at ¶ 61.) These conclusory assertions directly contradict the plain disclosure of Krishna. (*See, e.g.*, Ex. C2 at Fig. 3; 8:39–40 ("Processed packet cells are reassembled into packets and sent off the chip by an output FIFO 318.").) These conclusory assertions, which are at odds with the plain disclosure of Krishna, do not raise a genuine issue of material fact for trial. *See Sitrick*, 516 F.3d at 1001. Moreover, at his deposition, Dr. Rubin admitted that Krishna in fact discloses this limitation. (Ex. C5 at 236:22–238:13.)

(f): "wherein each of the plurality of processors is adapted to generate its respective output information based at least in part on the control parameters and the cryptographic parameters, and the output data is a cryptographic processing result"

Krishna discloses that each of the "plurality of processors" (cryptographic processing engines 316) is adapted to generate its respective "output information" based at least in part on the "control parameters" and the "cryptographic parameters," so that the "output data" is a "cryptographic processing" result. For example, the "control unit" (packet classifier 304) determines "security association information' required to process the packet, such as "encryption keys, data, etc." (Ex. C2 at 7:63–67; *see also id*. at 5:54–57; Ex. C5 at 235:7–236:10, 244:23–245:6; Blaze Decl. ¶¶ 18, 27.) This security association information includes at least one "control parameter" (e.g., "u32 byteCount," which identifies the "[t]otal payload bytes processed via this entry") and at least one "cryptographic parameter" (e.g., "cryptoState algoCrypto," which identifies "[k]eys and other parameters for crypto," or "u8 crypto:2," which identifies the type of encryption or decryption, such as "DES, 3DES, RC4, NONE"):



The structures are accessed by SA index, as generated by the packet classifier.

Partial contents for the SA Auxiliary structure are as shown in the following C code fragment:

```
typedef struct SATAux__struct {
      u32 byteCount;              /* Total payload bytes processed via */
                                  /* this entry (larger of crypto or auth bytes) */
      u64 expiry;                 /* Expiry time or #bytes for this */
                                  /* entry (checked per use) */
      u32 packetCount;            /* Stats - # packets processed via this entry */
      struct SATAux__struct *next;       /* Next IPSec Security Association for SA */
                                                /* bundles */
      u32 seqNoHi;                /* Anti replay sequence number - "right" edge of window */
                                  /* for outgoing packets, used for next sequence number */
      u64 seqWin;                 /* Anti-replay sequence window (bit mask) */
      u32 peerAddr;               /* IPSec peer security gateway address */
      u32 spi;                    /* IPSec security parameter index */
      u8 originalProtocol;/* pre-IPSec Protocol to which this SA applies */
      cryptoState algoCrypto;       /* Keys and other parameters for crypto */
      authState algoAuth;             /* Keys, state and other HMAC parameters */
      u8 enableSeq:1;             /* 1 to enable anti-replay sequence check */
      u8 crypto:2;                /* DES, 3DES, RC4, NONE */
      u8 auth:2;                  /* MD5, SHA1, NONE */
      u8 format:2;                /* FORMAT__ESP, FORMAT__AH, FORMAT__AH__ESP */
      u8 tunnel:1;                /* 1 to enable tunneling, 0 to use transport adjacency */
      u8 discard:1;               /* Drop packet */
      u8 pass:1;                  /* Pass packet through */
      u8 intr:1;                  /* Interrupt upon match to this entry */
                                  /* (useful for drop/pass) */
      u8 explicitiv:1;            /* Use implicit IV from SAdB as opposed to explicit */
                                  /* IV from packet */
      u8 padnull:1;               /* Apply pad to 64-byte boundary for ESP */
                                  /* null crypto upon IPSec output */
      u8 oldpad:1;                /* Old style random padding per RFC1829 */
} SATAux;
```

(Ex. C2 at 14:1–35; *see also* Ex. C5 at 221:11–222:22; Blaze Decl. ¶ 28.) This security association information is sent to each of the "plurality of processors" (cryptographic processing engines 316) for security processing via the packet distributor 306. (Ex. C2 at 8:10–17; *see also id*. at 6:1–9; Ex. C5 at 236:11–15; Blaze Decl. ¶ 29.) The "output data" is an encrypted or decrypted data packet, *i.e.*, a "cryptographic processing result." (Ex. C2 at Abstract; 2:12–18; 3:66–4:13; *see also* Ex. C5 at 238:2–13; Blaze Decl. ¶ 29.)

In his expert report, Dr. Rubin denied that Krishna discloses this claim element, but did not provide any support for his denial, stating without explanation that "the processors of

Krishna '131 do not generate respective output information based on control parameters and crypto parameters." (Ex. C4 at ¶ 62.) Such a conclusory assertion, which is at odds with the plain disclosure of Krishna as discussed above, does not raise a genuine issue of material fact for trial. *See Sitrick*, 516 F.3d at 1001. Moreover, Dr. Rubin admitted at his deposition that Krishna discloses this limitation. (Ex. C5 at 236:22–237:4.)

There is thus no genuine issue of material fact that Krishna discloses each and every limitation of claim 1 of the '448 patent.

2. Krishna Discloses Every Element Of Claims 2–9.

For similar reasons set forth above for claim 1, Krishna also discloses every element of dependent claims 2–9 of the '448 patent. (Ex. C3.) In his expert report, Dr. Rubin denied that Krishna discloses the additional limitations required by these claims, but provided no support for his denials. (Ex. C4 at ¶¶ 63–69.) Such conclusory assertions, which are at odds with the plain disclosure of Krishna as discussed below, do not raise a genuine issue of material fact for trial. *See Sitrick*, 516 F.3d at 1001.

Claim 2: "The system of claim 1, wherein said control unit is further adapted to provide state data representative of a state of the processor array"

Krishna discloses that the "control unit" (packet classifier 304) provides "state data representative of a state of the processor array." For example, Krishna discloses that state information is included as part of the "security association information" provided by the "control unit" (packet classifier 304). (Ex. C2 at 14:1–35 (describing "security association information" as including "authState algoAuth" which identifies "[k]eys, state and other HMAC parameters," and "cryptoState"); *see also id*. at 8:36–38 ("A status buffer 310 may be used to store processing status information, such as errors, etc."); Blaze Decl. ¶ 33.)

Claim 3: "The system of claim 1, wherein the main data is encrypted data and the output data is decrypted data"

Krishna discloses that the "main data" may be encrypted data and that the "output data" is decrypted data. For example, Krishna explains that the system can be used to both encrypt and decrypt data packets. (Ex. C2 at 3:66–4:3; Blaze Decl. ¶ 35.) Additionally, Fig. 6A illustrates using the Krishna system to decrypt an encrypted input packet so that that "output data" is decrypted data (e.g., a "clear text packet"). (Ex. C2 at Fig. 6A, 12:60–13:5; Blaze Decl. ¶ 36.)

Claim 4: "The system of claim 1, wherein the main data is unencrypted data and the output data is encrypted data"

Krishna discloses that the "main data" may be unencrypted data and that the "output data" is encrypted data. For example, Krishna explains that the system can be used to both encrypt and decrypt data packets. (Ex. C2 at 3:66–4:3; Blaze Decl. ¶ 38.) Additionally, Fig. 6B illustrates using the Krishna system to encrypt an unencrypted input packet so that the "output data" is encrypted data (e.g., an "encrypted packet"). (Ex. C2 at Fig. 6B, 13:36–49; Blaze Decl. ¶ 39.)

Claim 5: "The system of claim 1, wherein each respective at least a portion of the main data is a multiplexed process stream"

As illustrated in Fig. 3, Krishna discloses a "first distributor" (packet distributor 306) adapted to receive the "main data" from the "format filter" (Input FIFO 302), and to distribute to each of the "plurality of processors" a respective at least a portion of the "main data":

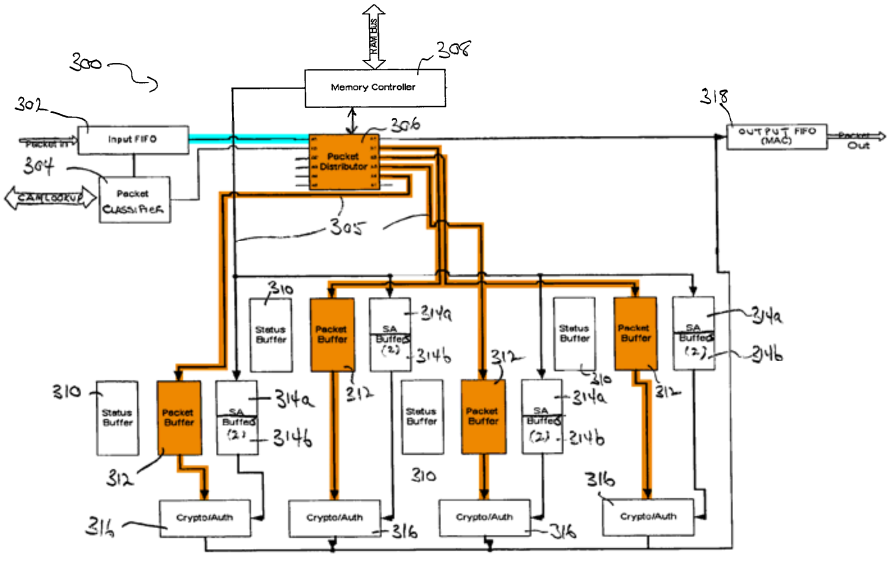


FIG. 3

(Ex. C2 at Fig. 3; Blaze Decl. ¶ 41.) As shown, "main data" (packet data) is sent from the "format filter" (Input FIFO 302) to the "first distributor" (packet distributer 306) over a single line. (Ex. C2 at Fig. 3; Blaze Decl. ¶ 42.) The packet distributor 306 then distributes each respective at least a portion of the packet data as a "multiplexed process stream" via the internal bus 305 among the plurality of cryptography processing engines 316. (Ex. C2 at 8:13–17; *see also id.* at 6:4–9; Blaze Decl. ¶ 42.) This is identical to the structure disclosed in the '448 patent. (Ex. C1 at Fig. 2.)

Claim 6: "The system of claim 1, wherein each of the plurality of processors is adapted to initialize based at least in part on the at least one respective control parameter received from the control unit"

Krishna discloses that each of the "plurality of processors" (cryptographic processing engines 316) is adapted to initialize based at least in part on the at least one respective "control parameter" received from the "control unit." For example, as discussed above, the security association information is distributed to each of the "plurality of processors." (Ex. C2 at 8:10–17; *see also id.* at 6:1–9; Ex. C5 at 236:3–15; Blaze Decl. ¶ 44.) The security association information includes at least one "control parameter" (e.g., "u32 byteCount") which identifies the "[t]otal payload bytes processed via this entry" to be used to initialize the processor. (Ex. C2 at 14:1–35; Ex. C5 at 221:11–222:3; Blaze Decl. ¶ 44.)

Claim 7: "The system of claim 1, wherein each of the plurality of processors is adapted to perform a cryptographic function based at least in part on the at least one respective cryptographic parameter received from the control unit"

Krishna discloses that each of the "plurality of processors" (cryptographic processing engines 316) is adapted to perform a cryptographic function based at least in part on the at least one "cryptographic parameter" received from the "control unit." For example, as discussed above, the security association information is distributed to each of the "plurality of processors." (Ex. C2 at 8:10–17; *see also id*. at 6:1–9; Ex. C5 at 236:3–15; Blaze Decl. ¶ 46.) The security association information includes at least one "cryptographic parameter" (e.g., "cryptoState algoCrypto," which identifies "[k]eys and other parameters for crypto") that in part controls the performance of the cryptographic function. (Ex. C2 at 14:1–35; Ex. C5 at 222:4–22; Blaze Decl. ¶ 46.)

Claim 8: "The system of claim 1, wherein the at least one respective cryptographic parameter is keying data"

Krishna discloses that the at least one "cryptographic parameter" may be "keying data." For example, the security association information includes at least one "cryptographic parameter" (e.g., "cryptoState algoCrypto," which identifies "[k]eys and other parameters for crypto"). (Ex. C2 at 14:1–35; *see also id.* at 7:63–67; Ex. C5 at 222:4–22; Blaze Decl. ¶ 48.)

Claim 9: "The system of claim 1, wherein at least one of the first distributor and the second distributor is a switching matrix"

As illustrated in Fig. 3 of Krishna, the "first distributor" (packet distributor 306) may be a "switching matrix":

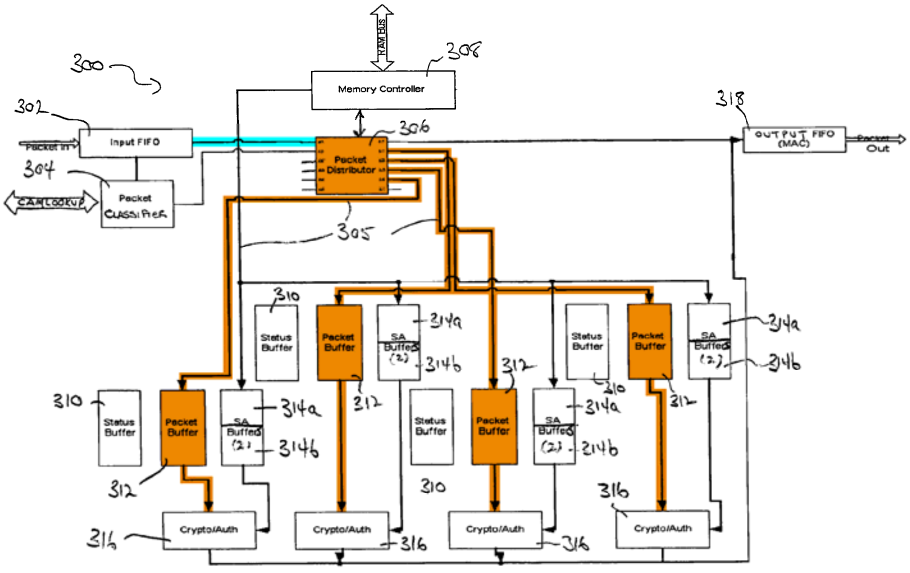


FiG. 3

(Ex. C2 at Fig. 3; Blaze Decl. ¶ 50.) For example, the packet distributor 306 receives data packets on a single line from Input FIFO 302 and then switches the data onto several lines for distribution to the "plurality of processors" (cryptographic processing engines 316). (Ex. C2 at 8:13–17; *see also id*. at 6:4–9; Blaze Decl. ¶ 50.)

3. Krishna Discloses Every Element Of Claims 10–18.

Claims 10–18 of the '448 patent include substantially the same limitations as claims 1–9, and are invalid for the reasons set forth above. (Ex. C1; Blaze Decl. ¶ 53.) For example, similar to claims 1–9, there is no genuine dispute that Krishna discloses each of the elements of claims 10–18 of the '448 patent, as set forth in the claim chart of Ex. C3. (Blaze Decl. ¶ 53.) TecSec's expert provides no basis for concluding otherwise. (Ex. C4.) These claims are thus invalid as anticipated under 35 U.S.C. § 102(e).

CONCLUSION

For the foregoing reasons, IBM respectfully requests that this Court grant its Motion for Summary Judgment of Inequitable Conduct and Invalidity.

Dated: November 15, 2010

Respectfully submitted,

/s/ Craig C. Reilly
Craig C. Reilly, Esq. (VSB # 20942)
111 Oronoco Street
Alexandria, Virginia 22314
Telephone: 703-549-5354
Facsimile: 703-549-2604
E-mail: craig.reilly@ccreillylaw.com
Counsel for Defendant IBM

Of Counsel for Defendant IBM:

John M. Desmarais
DESMARAIS LLP
230 Park Avenue
New York, NY 10169
Telephone: 917-340-6940
Facsimile: 914-666-6962

Jon T. Hohenthaner
Jeanne M. Heffernan
KIRKLAND & ELLIS LLP
601 Lexington Avenue
New York, NY 10022-4675
Telephone: 212-446-4800
Facsimile: 212-446-4900

Elizabeth Bernard
KIRKLAND & ELLIS LLP
655 15th Street, N.W.
Washington, D.C. 20005
Telephone: 202-879-5000
Facsimile: 202-879-5200

CERTIFICATE OF SERVICE

I hereby certify that on this 15th day of November 2010, a true and correct copy of the foregoing pleading or paper was served using the Court's CM/ECF system, with electronic notification of such filing to the following counsel of record:

Brian M. Buroker
HUNTON & WILLIAMS
1900 K Street NW
Washington, DC 20006-1109
Telephone: 202-955-1500
Facsimile: 202-778-2201
E-mail: bburoker@hunton.com
Counsel for Plaintiff

/s/ Craig C. Reilly
Craig C. Reilly, Esq. (VSB # 20942)
111 Oronoco Street
Alexandria, Virginia 22314
Telephone: 703-549-5354
Facsimile: 703-549-2604
E-mail: craig.reilly@ccreillylaw.com
Counsel for Defendant IBM